POL00423694

Agenda

POST OFFICE LIMITED

Meeting:	Risk and Compliance Committee
Date:	12 January 2021
Time:	10.00 - 13.00
Location:	Via Microsoft Teams

Present:	**Attendees:**
Alisdair Cameron (Chair)	Johann Appel (Head of Internal Audit)
Lisa Cherry (Group Chief People Officer)	Mark Baldock (Head of Risk)
Ben Foat (Group General Counsel)	Jonathan Hill (Compliance Director)
Amanda Jones (Group Retail and Franchise Network Director)	Tom Lee (Head of Finance Financial Accounting and Controls)
Cathy Mayor (Finance Director, Commercial)	Rebecca Whibley (Senior Assistant Company Secretary)
Jeff Smyth (Group Chief Information Officer)	Rob Wilkins (Cloud Services Director): Item 3.4 & 4
	Tony Jowett (Chief Information Security Officer): Items 4 & 5
	Russell Hancock (Supply Chain Director): Item 6
	Sally Smith (Money Laundering Reporting Officer & Head of Financial Crime): Item 7
	Maxine Cross (Head of Reward and Pensions): Item 8
	Helen Rhodes (Head of HR Organisation Effectiveness Project Lead): Item 8
	Brian Kelly (Director - Tax, Treasury and Working Capital): Item 9
	Andy Jamieson (Head of Tax) – Item 9
	Tim Perkins (Service and Support Optimisation Director): Item 10, 11 & 12
	Declan Salter (GLO Director): Item 13
	Graham Hemmingway (Historical Matters Portfolio Lead): Item 13
	Barbara Brannon (Procurement Director): Item 16
	Sarah Gray (Group Legal Director): Item 17
Apologies:	

Dial In Details:

Join Microsoft Teams Meeting

GRO United Kingdom, London (Toll)

Conference ID: GRO

Pin (if applicable): GRO

Time		**Item**		**Owner**	**Action**
10:00	1.	Welcome & Conflicts of Interest		Chair	Noting
10.05	2.	Previous Meetings		Chair	
		2.1	Minutes (12 November 2020)		Approval
		2.2	Actions List		Discussion
	3.	Combined Risk, Compliance and Audit Update			
10:10		3.1	Risk Update	Mark Baldock	Noting & Approval (onward submission to ARC)
10:20		3.2	Risk Appetite Statement: Legal, Compliance & Governance	Ben Foat & Jonathan Hill	Approval (onward submission to ARC)
10:25		3.3	Compliance Update	Jonathan Hill	Noting & Approval (onward submission to ARC)
10:35		3.4	Internal Audit Update	Johann Appel (& Rob Wilkins)	Noting & Approval (onward submission to ARC)

POL00423694

POST OFFICE LIMITED

	4.	PCI-DSS and Cyber Security Update			
10:45		4.1	PCI-DSS	Jeff Smyth & Rob Wilkins	Noting
10:50		4.2	Cyber Security	Tony Jowett	Noting (onward submission to ARC)
10:55		4.3	Joiners, movers, leavers	Tony Jowett	Noting (onward submission to ARC)
11:00	5.	IT Controls Assessment		Tony Jowett	Noting (onward submission to ARC)
11:10	6.	Supply Chain Historical IT Risks		Russell Hancock	Noting
11:20	7.	Money Laundering Annual Report		Sally Smith	Discussion & Approval (onward submission to ARC)
	8.	HR Update:			
11:50		8.1	Pensions Controls	Lisa Cherry & Maxine Cross	Noting (onward submission to ARC)
11:55		8.2	Success Factors	Lisa Cherry & Helen Rhodes	
12:00	9.	Tax Update & Tax Strategy		Brian Kelly & Andy Jamieson	Noting & Approval (onward submission to ARC)
12:05	10.	Update on branch losses and balances on Postmaster accounts		Tim Perkins	Noting (onward submission to ARC)
12:10	11.	Postmaster Policies - Postmaster Account Support Policy - Postmaster Accounting Dispute Resolution Policy - Network Monitoring and Audit Support Policy		Tim Perkins	Approval (onward submission to ARC)
12:20	12.	Mails Fraud Update		Tim Perkins	Noting (onward submission to ARC)
12:25	13.	Historical Matters Unit: Fraudulent Claims Controls & Delegation of Authority		Declan Salter & Graham Hemmingway	Noting (onward submission to ARC)
12:35	14.	Policies for Approval:		Jonathan Hill	Approval (onward submission to ARC)
		14.1	Summary Paper		
		14.2	Cyber & Information Security		
		14.3	Investigations		
		14.4	Employee, Postmaster & Postmaster Assistant Vetting Requirements		
12:45	15.	Subsidiary Policy Mandate		Jonathan Hill	Approval

Strictly Confidential

POL00423694

POST OFFICE LIMITED

				(onward submission to ARC)
12:50	16.	Procurement Compliance & Governance	Barbara Brannon	Noting (onward submission to ARC)
12:55	17.	Law & Trends Update	Sarah Gray & Ben Foat	Noting (onward submission to ARC)
13:00	18.	Review of draft Audit, Risk and Compliance Committee (ARC) meeting agenda 26 January 2021	Chair	Noting
	19.	Any other business	Chair	Noting
Next Risk & Compliance Meeting: Tuesday 16 March 2021 at 10.00 - 13.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ				

POL00423694

2.1

POST OFFICE LIMITED

MINUTES OF A MEETING OF THE RISK AND COMPLIANCE COMMITTEE OF POST OFFICE LIMITED HELD ON THURSDAY 12 NOVEMBER 2020 AT 11:00 VIA MICROSOFT TEAMS

Present:	**Attendees:**
Alisdair Cameron (Chairman) **(AC)**	Helen Rhodes (People Shared Services Director) (observing) **(HR)**
Lisa Cherry (Group Chief People Officer) **(LC)**	Meredith Sharples (Director of Telecoms) **(MS)**: Item 3.3
Ben Foat (Group General Counsel) **(BF)**	Tony Jowett (Chief Information Security Officer) **(TJ)**: Item 4
Amanda Jones (Group Retail and Franchise Network Director) **(AJ)**	Rob Wilkins (Cloud Services Director) **(RWI)**: Item 4
Cathy Mayor (Finance Director, Commercial) (deputising for Owen Woodley) **(CM)**	Mark Underwood (LCG Operations Director) **(MU)**: Item 5
Jeff Smyth (Group Chief Information Officer) **(JS)**	Tim Perkins (Head of Security, Safety & Loss Prevention) **(TP)**: Item 6
Regular Attendees:	Christine Kirby (Financial Controls Manager) **(CK)**: item 7
Johann Appel (Head of Internal Audit) **(JA)**	Brian Kelly (Finance Director - Tax, Treasury and Working Capital) **(BK)**: Item 8
Mark Baldock (Head of Risk) **(MB)**	Declan Salter (GLO Director) **(DS)**: Item 9
Jonathan Hill (Compliance Director) **(JH)**	Graham Hemingway (Historical Matters Portfolio Lead) **(GH)**: Item 9
Tom Lee (Head of Finance Financial Accounting and Controls) **(TL)**	Ed Dutton (Post Office Insurance Managing Director) **(ED)**: Item 10
Rebecca Whibley (Senior Assistant Company Secretary) **(RW)**	Karl Oliver (Head of Commercial Partnerships) **(KO)**: Item 12
Apologies:	Dan Zinner (Group Chief Strategy and Transformation Officer) **(DZ)**: Item 13
Owen Woodley (Group Chief Commercial Officer) **(OW)**	Saira Burwood (Head of SPO) **(SB)**: Item 13
Nick Read (Group CEO) **(NR)**	Andrew Goddard (Payzone MD) **(AG)**: Item 14
	Sarah Gray (Group Legal Director) **(SG)**: Item 15
	Rod Williams (Head of Legal, DR & Brand) **(RWIL)**: Item 16
	Barbara Brannon (Procurement Director) **(BB)**: Item 17
	Ed Dyer (Working Capital and Cash Management Lead) **(EDY)**: Item 19

1.	**Welcome and Conflicts of Interest**	**Action**
	The Chair opened the meeting and advised that all papers would be taken as read. No conflicts of interest were declared.	
2.	**Minutes and Action Lists**	
2.1	The minutes of the Committee meeting held 10 September 2020 were **APPROVED**, subject to an amendment to paragraph 3.3 requested by Ben Foat such that it reads: *"Legal – POL unable to comply with legislative and regulatory changes, resulting in fines, lost revenue, reputational and customer damage. It was noted that legal and regulatory changes are managed through the Law & Trends forum and reported to RCC and ARC to avoid this."*	
2.2	Progress on completion of actions as shown on the action log was **NOTED** as follows: Action 1 from 10 September 2020 para 3.6 GLO/Freedom of Information Requests/GDPR: This action was covered the Data Governance item (see paragraph 16). The action was closed.	

DRAFT

	Action 2 from 10 September 2020 para 4 Pensions Assurance: Project Assurance Steerco has been created and was to meet monthly. Data was being recalculated and results would not be available until the end of November. An update would be provided to the Committee in January 2021. The action remained open. Action 3 from 13 July 2020 para 7 Suspense Accounts: This action was covered the Suspense Accounts item (see paragraph 5). The action was closed. Action 4 from 13 July 2020 para 3.5 Compliance Report (TelCo): An update was included in the Compliance Paper presented to the Committee. There was an error in the minutes for 13 July 2020 and the action should read: "*the Telco team was asked to consider ways to reduce the number of customers out of contract and to revert to the Committee with a statement/plan for November* ." The action remained open. Action 5 from 5 May 2020 para 3.15 Fit & Proper Policy: This policy would be presented to the Committee in January 2021 and HR have discussed involvement with Operations and it was agreed the policy was to be owned by Operations. The action was closed. Action 6 from 7 November 2019 para 10.6 MRLO Report: HMRC were still not conducting any meetings and the action was to be updated at the next meeting in January 2021. The action remained open. Action 7 from 7 November 2019 para 3.2 Supplier Contracts Out of Governance (SSK): SSK Procurement Project would now be formally closed and any future activity would sit under the Network Strategy workstream. Automation forms a clear part of this strategy and was fully backed by the Board. Network Strategy was due to go back to Board in January with an update on Automation and Technology (this included SPM dependencies and route to procure). In relation to the existing estate the procurement team were investigating a PCR compliant route to maintain the current estate and potential procurement of new with a target resolution date of 29/01/2021. The action remained open. Action 8 from 7 November 2019 para 3.3 Supplier Contracts Out of Governance (Brands/RAPP): A compliant tender process has been run and the contract has been awarded to the incumbent provider, with operational costs reduced. Contracts were nearing finalisation with a target completion date of end November. The action remained open. Action 9 from 7 November 2019 para 5.3 Cyber Security Incident Test: A desktop exercise to bed in new processes would be conducted in November and then in subsequent months an external party (Nettitude) would be used to conduct live tests. This action would otherwise be updated as part of the regular updates to the Committee. The action was closed.	
3.	**Risk, Compliance and Audit Update**	
	Risk	
3.1	Risk Dashboard: Mark Baldock introduced the paper, which had been circulated previously and was taken as read. In response to questions from the Committee, it was explained that the enterprise risk structure mirrors the Orange Book of Risk Management and was thematic. It was not expected that the risks would change from one month to another. It was the linked risks where the detail changed more frequently: there have been 72 new linked risks over the last three months and 100 linked risks were closed at an intermediate and local level. The question was when the changes in these linked risks impacted the enterprise risk and there needed to be	

POL00423694

	a material change to impact the enterprise risk rating. The Chair highlighted that the dashboard needed to better highlight any changes in risk vs. the ongoing management of an existing risk. Ben Foat further commented that risk scores were given but the numbers were not defined. It was also highlighted that Declan Salter should be identified against the GLO risk and the impact score for the Starling and GLO risk should be five, not three. It was agreed that Mark Baldock would make these changes to the risk dashboard, including putting any new risks to the front of the dashboard moving forwards (from January 2021) and provide a verbal update on these elements to the Audit, Risk & Compliance Committee (ARC) in November. The Committee otherwise **NOTED** the Risk Dashboard for onward submission to the Audit, Risk & Compliance Committee (ARC).	**Action: MB**
3.2	Risk Policy: The Committee approved the Risk Policy, incorporating the approach to Risk Appetite, for onward submission to the ARC, subject to the following changes: - Compliance was to be added to the second line of defence. - It was to be made clear that the policy applied to the Historical Matters Unit (HMU). - The Board and ARC were not first line defence entities but sat above the defence line structure so should be removed as first line defence entities. - The Committee was the be added to the Risk Governance Structure. - The operational detail included on page 13 would be taken out placed in the Risk Management Framework such that it could be changed if needed without needing to revise the policy. It was also confirmed that the policy did not apply to Payzone Bill Payments Limited and Post Office Insurance, although these entities will have regard to the policy. Both were to adopt their own Risk Policies and despite Post Office Insurance having its own ARC, the Group ARC still oversaw both entities with reports from Post Office Insurance to the Group ARC. Material risks for Post Office Insurance were also included in the Risk Dashboard.	**Action: MB**
	Compliance	
3.3	Jonathan Hill introduced the paper, which had been circulated previously and was taken as read. The specific items below were highlighted and discussed by the Committee. Telecoms Comms Incident: Jonathan Hill confirmed that this was the fourth or fifth regulatory breach seen in the Telecoms area. Whilst it was serious, the number of customers impacted was low and it was hoped the penalty would be minimised. It was not clear how much the fine could be as it could be up to 10% of revenue but it was expected to be less than the fine for the Text Rely issue which was £175,000 as the present incident was not as serious, took less time to resolve and affected less customers. Meredith Sharples explained that the breach was caused by a Fujitsu system failure attributed to file size issues. The breach protocol was immediately instigated and the team engaged with Ofcom. The number of customers impacted was small and the team was working to recompense. Fujitsu were to bear the cost for the breach and a proposal was expected from them later this week. The Chair congratulated Meredith Sharples on dealing with the issue quickly but highlighted that the current contractual situation was untenable (the contract and systems were seven years old and there was no appropriate compliance team). Ultimately, what happens next depended on the on-going strategic discussions regarding the possible sale of the Telecoms business. Branch registration errors: In response to questions from the Committee, it was confirmed that it was hoped there may little or no penalty for branches completing Travel Money transactions after having been de-registered from HMRC.	

POL00423694

	Money Service Business/Capita: It has been identified that high risk suspicious cash deposits from a Money Service Business (a money transmitter) were being accepted, via the bill payment reseller client Capita. The Chair highlighted that a decision had been taken to not use Money Service Businesses and therefore this practice must stop as soon as possible. Jonathan Hill explained that he was meeting with Capita next week (w/c 16 November 2020) and that they would be told to stop and a timeline would be agreed. Jonathan Hill indicated that the business would be seeking immediate termination and the Chair agreed with this approach. Compliance Monitoring: The Chair questioned whether it was right to pause mystery shopping due to the recent lockdown measures. Jonathan Hill explained that the decision was taken partly for safety (so mystery shoppers did not have to travel and go into branches), but also because no one was buying travel insurance due to the lockdown. As such, mystery shopping would recommence when travel was permitted. Anti-bribery and Corruption Training: It was explained that completion by the HR business unit was at 81.7% (compared to 96.5% across the business) (subject to revised figures being provided). Lisa Cherry was asked to ensure colleagues in her area completed this training as soon as possible and Jonathan Hill would provide her with the latest list of those who had not yet completed it. Whistleblowing Update: There were no thematic concerns and it was explained that the majority have been received from agent assistants and relate to allegations concerning Postmaster activity. A more centralised approach to Postmaster reported concerns was being taken (separate from the whistleblowing process) so as to ascertain any broad themes. Access to Cash: The Committee asked that the draft of the responses to the call for evidence on Access to Cash were circulated to the Group Executive (GE).	**Action: LC/JH** **Action: JH**
	Internal Audit	
3.4	Johann Appel introduced the paper, which had been circulated previously and was taken as read. The specific items below were highlighted and discussed by the Committee. Controls over Manual Revenue Adjustments: It was confirmed that third party data feeds were part of a separate audit planned for January 2021. The present audit has looked at manual revenue adjustments as a result of third party data but the team has not yet validated the third party data processes. Effectiveness of the Second Line during COVID-19: Ben Foat questioned whether the work being undertaken to put a Controls Framework in place was happening quick enough, noting there had been some delays in getting the project to the Project Review Board. The audit report emphasised that there could not be any more delays. It was agreed that this work should be taken to GE to discuss the need to develop the Framework and the approach that should be taken. Joiners, Movers & Leavers (JML): The Chair stressed the importance of completing this work. The risks for internal movers needed to be mapped and resolved. Lisa Cherry was asked to take this away. Further actions were also highlighted as needed to be completed prior to the report being submitted to the ARC:	**Action: RW (agenda) /JA/BF** **Action: LC**

POL00423694

	- The addition of Dan Zinner's comment to the Branch Hub (Programme Assurance) summary. - On the outstanding data privacy (document retention) action, it needed to be explained why the 31 October date had not been deliverable and what the new date was. If the issue could not be remedied, there needed to be detail as to what controls would be put in place. This should also be reflected in the Data Governance paper (see paragraph 16). Further, it was requested that: - Johan Appel send the headline details of the Special Investigation to the Chair. - Ben Foat and Jeff Smyth discuss offline the rules around deleting/not deleting data for legal reasons. The Committee otherwise **NOTED** the Combined Compliance and Internal Audit updates for onward submission to the ARC.	**Action: JA** **Action: JA/JS** **Action: JA** **Action: BF/JS**
4.	**PCI-DSS and Cyber Security Update**	
	PCI-DSS Programme Update	
4.1	Jeff Smyth introduced the paper, which had been circulated previously and was taken as read. IN response to questions from the Committee, it was confirmed the Ingencio **IRRELEVANT** Fujitsu worked on a time/materials basis and the programme has previously signalled a £1.2m cost risk to the ARC. The team were now requesting some changes to the solution so more funding would be required and this was presently being costed. However, the programme was making good progress and was hitting its milestones. It was on track to go through accreditation and the payment solution had already passed accreditation with Global Payments. The Committee otherwise **NOTED** the PCI-DSS Programme Update for onward submission to the ARC.	
	Cyber Security	
4.2	Tony Jowett introduced the paper, which had been circulated previously and was taken as read. The Committee raised concerns about the number of people who had skipped the phishing training (178) and had been lured by the fake phishing campaign (391). It was explained that the numbers tended to go up and down a little, but ultimately, there was no real progress and as such the team were doing a deeper root cause analysis. The "volume" would also be "turned up" on the phishing comms. It was also highlighted that phishing has continued to be more prevalent in the external environment, particularly with COVID-19 scams. It was requested that Tony Jowett provide a list of all individuals who have not done the training to the relevant GE members. Jeff Smyth and Lisa Cherry also agreed to flag the need for comms with Nick Read and highlight the issue with the Leadership Group. Tony Jowett was further asked to update the paper for the ARC reflecting the action that was being taken. Tony Jowett also noted that his team were looking at tool to monitor culture shift and it was agreed that he would liaise with HR on the on-going culture work to build this into the business' longer term defence plans. The Committee otherwise **NOTED** the Cyber Security Update for onward submission to the ARC.	**Action: TJ** **Action: JS/LC** **Action: TJ** **Action: TJ/LC**
	Joiners Movers Leavers (JML)	
4.3	Tony Jowett introduced the paper, which had been circulated previously and was taken as read. At the request of Jeff Smyth, Johann Appel confirmed that the work undertaken was on track with the current roadmap, but that the roadmap was incomplete and needed updating as part of an outstanding audit action. The highest exposure areas were being prioritised (leavers and movers) due to the recent organisational design work. Lisa Cherry confirmed that all processes for leavers and movers were being reviewed to ensure all bases were covered and Tony Jowett and	

DRAFT

POL00423694

	Helen Rhodes have weekly meetings with further regular touchpoints between the relevant teams. The regular list of leavers shared with IT has been expanded to include those at risk of redundancy such that this could also be monitored proactively. Tony Jowett was asked to put the detail relating to the focus on leavers and movers in the summary section of the paper for the ARC. The Committee otherwise **NOTED** the paper for onward submission to the ARC.	**Action: TJ**
	Belfast Data Center (Horizon) Disaster Recovery Post Test Briefing	
4.4	Gary Walker introduced the paper, which had been circulated previously and was taken as read. It was explained that each year the business is required to test disaster recovery at the Data Center in Belfast and this took place in August 2020. The test was partially successful with most transactions (48/52) being able to be traded out of the secondary site. Three transaction types failed and had to use the primary site. Post testing, the team have identified all root causes and implemented fixes. Smaller tests have then been carried out to check the fixes have worked. The current plan was to not to do another test of this size and scale this financial year but to ensure that as part of Belfast Exit there was equivalent activity in suitable point i.e. latter point of the next calendar year. The Chair commented that this was one of the business' biggest risks and felt that another test should be done at Easter given the recent test was only partially successful. Jeff Smyth explained that the test was expensive (circa £75,000) and also destroys all change programme activity hosted in the secondary data center. The Chair noted that £75k was a tiny sum compared to the cost and reputational damage of losing branch trading. It was agreed that the GE should agree the timing of the next test. The Committee otherwise **NOTED** the paper for onward submission to the ARC.	**Action: RW (agenda) GW**
5.	**Suspense Accounts**	
	Mark Underwood introduced the paper, which had been circulated previously and was taken as read. In response to questions from the Committee, it was outlined that since submission of the paper advice had been received from HSF and Peters & Peters. This confirmed that the outcome of the review of suspense accounts did not mean that the Historical Shortfalls Scheme needed to be altered, but that investigators could consider issues relating to Moneygram and cheques. The Chair questioned whether the KPMG report could and should be published. Mark Underwood explained that a decision could be taken to disclose the entire report or a redacted version. There was a question around the extent to which the report and its findings could trigger disclosure obligations, although the vast majority of the report was not disclosable. Mark Underwood was requested to ask the GE whether they wished the report to be fully disclosed or a redacted version. (*Post meeting note: Mark Underwood has advised that the ARC would be asked to discuss whether the KMPG report should be disclosed at its November 2020 meeting*). In conclusion, Mark Underwood explained that KPMG's view was that any further investigation would not uncover anything more and as such no further work on this topic was recommended. The Committee otherwise **NOTED** the report for onward submission to the ARC.	**Action: RW (agenda) MU**
6.	**Notification of Transaction Correction error**	
	Tim Perkins introduced the paper, which had been circulated previously and was taken as read. It was explained that an individual had posted transaction corrections without authorisation. The issue had been resolved and work was being undertaken to deal with the individual involved and discussions were being had with Accenture to see if a failsafe could be put in place to prevent this happening action. It was agreed that the outcome of the investigation into the error should be published in the interests of transparency (Tim Perkins to arrange). The Committee otherwise **NOTED** the paper.	**Action: TP**
7.	**Financial Reporting Controls Framework Update**	

DRAFT

POL00423694

	Tom Lee introduced the paper, which had been circulated previously and was taken as read. The Committee noted that there were no concerns highlighted in the report and **NOTED** the paper for onward submission to the ARC.	
8.	**Agreed Upon Procedures**	
	Tom Lee introduced the paper, which had been circulated previously and was taken as read. The Committee challenged the number of findings in the Note Circulation Scheme (NCS) area. Tom explained that the bulk of these related to evidence that was not available due to COVID-19. The remaining issues were not major concerns and had been shared with Bank of England, who were comfortable with the findings. A detailed action plan has been set up and would be fully implemented by the end of the month. Tom Lee was asked to include these points in the executive summary section of the report. The Committee otherwise **NOTED** the report for onward submission to the ARC.	**Action: TL**
9.	**Historical Matters Unit (HMU) Governance Review**	
	Graham Hemmingway and Declan Salter introduced the paper, which had been circulated previously and was taken as read. It was explained that much progress had been made to set up the Governance of the new HMU, but it was not yet finalised. It was noted that this should be made clear in the paper to the ARC. Further Ben Foat explained that the HMU would follow the usual business policies and would only have an exemption in terms of litigation. Notably Post Office has not signed up to the Crown Services legal panel so this should be corrected. It was further noted that work was ongoing to address the backfill and funding as business-as-usual resource was continuing to support the HMU. The Committee otherwise **NOTED** the paper for onwards submission to the ARC.	**Action: GH**
10.	**Post Office Insurance Financial Conduct Authority Dual Pricing Change Impact**	
	Ed Dutton introduced the report, which had been circulated previously and was taken as read. It was explained that the recent prohibition on "Price Walking" (competitive new business prices followed by renewal prices increasing during contract) in Motor and Home Insurance blows the traditional insurance business model out the water and fundamentally means you cannot charge new customers different prices to existing customers. It was expected that this prohibition would come into other markets in due course. Post Office Insurance was still working through what this meant for the business, but it was thought that there would still be opportunities for competition as there would still be different views as to what a customer would cost. A new business policy would also have a positive value, unlike before. There were also strict rules on avoidance, but you can give vouchers for money off. The Chair requested that the piece be brought back to the GE in due course from a commercial and strategic perspective. At present, Post Office Insurance was still working through what the changes meant for them and a Board Committee was being set up. The impact would be clearer by January 2021. The Committee otherwise **NOTED** the paper for onward submission to the ARC.	
11.	**Committee Terms of Reference**	
	The Chair introduced the paper which had been circulated previously and was taken as read. The Committee **APPROVED** the draft Terms of Reference for onward submission to the GE, subject to the following amendments: - It should be specifically called out that the Committee has oversight of the HMU; and - The membership should be updated to include: Alisdair Cameron, Ben Foat, Jeff Smyth, Lisa Cherry, Amanda Jones and Cathy Mayor.	**Action: RW**
12.	**Deepdive: Multiple Partner financial stability update**	
	Amanda Jones introduced the paper, which had been circulated previously and was taken as read. In response to questions from the Chair, it was explained that the use of an external consultant was considered to provide insight as to what was really	

	happening in a particular organisation vs. what can be ascertained from information in the public domain. This was support with looking at trading statements and brokers to help the business synthesise this information. The Chair was sceptical that this would make much difference, but agreed that it could be used to show early "red lights." Amanda Jones further explained that small retailers had done better than expected during the COVID-19 crisis. However, WH Smiths were having some difficulties but thought they were financially strong and well placed to recover. They have announced 25 high street closures, including six Post Offices. The business was already aware of two of these. There was likely to be some noise around these as they were recent franchises (Amanda Jones was asked to check the legal position regarding WH Smith closing recently franchised branches). WH Smith had also indicated that there were IRRELEVANT and they have negotiated with their landlords to get a IRRELEVANT They have indicated there would be IRRELEVANT Furthermore, new core hours have been formalised from January 2021 and the plan was to maintain these hours rather than see more closures. The Committee otherwise **NOTED** the paper for onward submission to the ARC.	**Action: AJ**
13.	**Deepdive: Transformation Office Change Update 2020**	
	Dan Zinner introduced the paper, which had been circulated previously and was taken as read. It was explained that the ARC had asked for programme update and specifically wanted to know more about the Change Controls Framework. Saira Burwood further outlined that the paper was seeking ARC support for the future work to ensure sponsors and project leads were aware of their obligations under the change lifecycle. Ultimately, the paper was an update on what had been achieved thus far and the focusses for the next few months. The Committee **NOTED** the paper and the only comment was that it might benefit from being shortened.	
14.	**Payzone Risk Report**	
	Andrew Goddard introduced the paper, which had been circulated previously and was taken as read. On the whole, the risk management in Payzone had improved and there was now a better culture alongside monthly reviews of risks. The only area of concern was network resilience (cyber security) and it was confirmed that Post Office It has not yet done a comprehensive review of the Payzone network, but Andrew Goddard explained there had been disaster recovery work done for its Vodafone datacentres. A "hack" into the system was scheduled but had been postponed due to COVID-19. Ben Foat noted the good progress Payzone had made with respect of adopting Group Policies and questioned what operational processes were in place to implement the policies. Andre Goddard confirmed that policy implementation was part of management responsibilities and policies were being built into ways of working, but the work was on-going. Mark Baldock further noted that work with the Payzone Risk team had also gone well and the team were using the Post Office GRC tool. The Committee otherwise **NOTED** the Payzone risk report for onward submission to the ARC.	
15.	**Law & Trends Update**	
	Ben Foat introduced the paper, which had been circulated previously and was taken as read. The main issue that was highlighted related to the HMRC announcement in September 2020 that VAT should be charged on settlement payments made to third parties. The impact of this on recent settlements made to Postmasters as part of GLO and otherwise was still being worked through and was further complicated by the fact that some Postmasters had been employees. There was a need to work through all settlement payments made since 2016. The Department of Business, Energy and Industrial Strategy (BEIS) and UKGI were already aware. The Committee otherwise **NOTED** the Law & Trends Update for onward submission to the ARC.	
16.	**Data Governance**	

POL00423694

	Jonathan Hill introduced the paper, which had been circulated previously and was taken as read. It was explained that the update was requested by the ARC after the 31,000 boxes came to light that were previously unknown to the wider business to consider the broader lens of data management and accountabilities. At present, the remediation plan was outlined, but the sampling of the boxes had not yet started. The challenge was the way Post Office currently structures its data and information The Committee felt that the business needed to be sure that there was no data that was otherwise unknown to the wider business being stored elsewhere. The following points were discussed: - The Committee requested that Procurement check that there are no other contracts for data storage or archiving other than those with the Postal Museum and Oasis. - Writing out to branches for data might not be successful but that Tracy Marshall (Postmaster Effectiveness Director) was to take ownership of these requests to branches and Jonathan Hill was already working with Tracy to agree how best to do this. - A Record Retention programme had been completed earlier this year and person was being undertaken to realign data owners to new roles. - An individual needed to be assigned to go into each admin building to check cupboards and rooms to ensure there was no data that was unknown. - Jeff Smyth highlighted that this work could never be complete unless electronic data was also considered (which would include digitising paper records and tagging appropriately). - Rod Williams explained that colleague's emails when they leave can be retrieved, but OneDrive data was harder to retrieve as this was deleted very quickly. There needed to be debate on what was kept and for how long considering data protection obligations. Accordingly, the Legal, Data Protection, IT and Ruk Shah (MI & Analytics Director) were asked to work on a coherent recommendation on how the data retention policy should evolve and how it will be implemented. This should return to the RCC and ARC in January 2021. Further, the current paper needed to articulate the next steps and process that will be worked through. The Committee otherwise **NOTED** the report and **APPROVED** the next steps of: - to complete the remediation activity on an expedited basis in coordination with the Post-Conviction Disclosure Exercise and Historical Shortfall Scheme Activity; - for the legal team to conclude the agreed actions in respect of the assessment of all boxes stored at Oasis, on behalf of Post Office; and - for the GE to agree overall data governance accountability; for onward submission to the ARC.	**Action: BB** **Action: JH** **Action: BF/JH/JS** **Action: JH**
17.	**Procurement Governance & Compliance Report**	
	Barbara Brannon introduced the paper, which had been circulated previously and was taken as read. The following points were highlighted: - End User Computer Services (EUC): the project was re-baselined and as a result the revised plan targeted April 2021, which was later than the date provided to the Board. The Public Contract Regulations (PCR) risk was unchanged but the exit service risk was higher and IT were looking at the plan. - Common Digital Platform (CDP): The tender process has slipped and at present the application support and development services were unlikely to have been completely retendered or moved to other existing PCR compliant contracts by December as proposed to GE and Board and there were concerns in respect of resourcing and funding.	

- Smith & Williamson: This contract was just being finalised with Finance and would be submitted to the Board.
- Audit Contract: A compliant extension option existed to extend but PWC were currently working at risk preparing an audit plan for 2020/21 while commercial terms are being negotiated.
- Cheque Clearing: (*Greg Lewis joined for this update only*) A risk exception was submitted to Board in June 2020 to IRRELEVANT our cheque clearing services with Barclays IRRELEVANT. The service was needed as Post Office has a IRRELEVANT IRRELEVANT and have obligation with DLVA to accept cheques until IRRELEVANT IRRELEVANT The recommendation was to complete an RFI before Christmas to understand the market and this would require a IRRELEVANT

IRRELEVANT

The Chair requested that these items should be covered in the paper for the Board, noting that the business needed to be as transparent as possible. The paper submitted to the Committee could be used, but should be cut down.

Action: BB

It was then explained that the ARC approved the following approach to Procurement Risk Exceptions in September 2020:

1. Subthreshold exceptions (<£189,000) would be retrospectively reported to RCC and ARC every two months. This will become a standing item at ARC rather than an annual report. ARC will review this position within 6 months.
2. Above threshold risk exceptions (>£189,000) would continue to require prior approval from Board
3. Above threshold Pipeline risks, sourcing options and recommendations, progress reports for material procurements, and bi-annual strategic pipeline report would continue to be reported to the Board.

Prior to March 2020, subthreshold exceptions were approved by the relevant GE member and SLP; and the Procurement Director. These exceptions were logged, with mitigation plans to bring into compliance where exceptions were made for an ongoing requirement rather than a one-off event. The Committee was asked what approach they now preferred for the subthreshold exceptions given the ARC approved approach. The Committee discussed the approaches including: RCC approval, continuing with GE, SLP and Procurement Director approval and GE approval. Ultimately, it was felt that the ARC approved approach was to instil more proactive and transparent behaviours and therefore having GE overnight would add value to the approach.

Accordingly, the Committee:

- **NOTED** the that no Procurement Risk Exceptions have been submitted to the Post Office Limited Board since September 2020 and the contracts in the Procurement pipeline;
- **APPROVED** the approach to the cheque processing contract and the proposed next steps as outlined, subject to this being included in the paper for the Board;
- **NOTED** the alteration in governance approved by the ARC; and
- **APPROVED** that GE should approve any subthreshold risk exception requests moving forwards at its monthly meetings.

Post meeting note: It was agreed with the Company Secretary that as the Board report on Procurement would be near identical to the ARC report that the report would

POL00423694

	only be presented to the ARC but would also be shared separately with Lisa Harrington as the only member of the Board not on the ARC.	

18.	**Policies for Approval:**	
	Jonathan Hill introduced the paper, which had been circulated previously and was taken as read. It was highlighted that the Freedom of Information (FOI) Policy was a new policy and a lot of work had been done to operationalise it. It had been developed as Information Commissioner's Office (ICO) Guidance recommended such a policy and it provided a framework for colleagues to help them understand the importance of FOI requests. Cathy Mayor flagged that the policy should include guidance on when FOI requests would not be granted and it was explained that this was dealt with under the roles and responsibilities section. It was also noted that the Committee felt Post Office had too many policies. As such, the following policies were **APPROVED** for onward submission to the ARC: • Change Management; • Conflicts of Interest; • Protecting Personal Data; and • Freedom of Information & Environmental Information Regulations.	
19.	**Directors & Officers Insurance Renewal**	
	Ed Dyer introduced the paper which had been circulated previously and was taken as read. It was confirmed that all insurance cover was now full yin place. The Chair congratulated Ed on his hard work, particularly as the commercial insurance market was very difficult at the moment. All cover is fully in place. The Committee otherwise **NOTED** the report for onward submission to the ARC.	
20.	**Review of draft Audit, Risk and Compliance Committee meeting agenda for 24 November 2020**	
	The draft ARC agenda for 24 November was **NOTED**.	
21.	**Any other Business**	
	There was no other business.	

DRAFT

POL00423694

Post Office Limited
Risk & Compliance Committee
OPEN ACTIONS

No.	Meeting Date	Minute Reference	Action	Action Owner	Due Date	Comment
1	12/11/2020	3.1 Risk Compliance & Audit Update	**Risk Dashboard**: The Chair highlighted that the dashboard needed to better highlight any changes in risk vs. the ongoing management of an existing risk. Ben Foat further commented that risk scores were given but the numbers were not defined. It was also highlighted that Declan Salter should be identified against the GLO risk and the impact score for the Starling and GLO risk should be five, not three. It was agreed that Mark Baldock would make these changes to the risk dashboard, including putting any new risks to the front of the dashboard moving forwards (from January 2021) and provide a verbal update on these elements to the Audit, Risk & Compliance Committee (ARC) in November.	Mark Baldock	March RCC & ARC 2021 ~~January RCC & ARC 2021~~	06/01/2021: These changes have not been made for January 2021 due to the Risk Team having moved off the RSA Archer system and are now building ServiceNow (IRM Pro) system. As such it is difficult to run Dashboards. The reporting in the new ServiceNow system will be built to take account of this action where possible. 30/11/2020: A verbal update was provided to the ARC as required.
2	12/11/2020	3.1 Risk, Compliance & Audit Update	**Risk Policy:** The Committee approved the Risk Policy, incorporating the approach to Risk Appetite, for onward submission to the ARC, subject to the following changes: -Compliance was to be added to the second line of defence. -It was to be made clear that the policy applied to the Historical Matters Unit (HMU). -The Board and ARC were not first line defence entities but sat above the defence line structure so should be removed as first line defence entities. -The Committee was the be added to the Risk Governance Structure. -The operational detail included on page 13 would be taken out placed in the Risk Management Framework such that it could be changed if needed without needing to revise the policy.	Mark Baldock	November 2020 ARC	30/11/2020: These changes were made and the policy was approved by the ARC at its meeting in November 2020. **Recommended for closure.**
3	12/11/2020	3.3 Risk, Compliance & Audit Update	**Compliance Update:** Anti-bribery and Corruption Training: It was explained that completion by the HR business unit was at 81.7% (compared to 96.5% across the business) (subject to revised figures being provided). Lisa Cherry was asked to ensure colleagues in her area completed this training as soon as possible and Jonathan Hill would provide her with the latest list of those who had not yet completed it.	Jonathan Hill/Lisa Cherry	ASAP with update to be provided @ January 2021 RCC	15/12/2020: Current HR figure stands at 92.4%, which includes contractors. Work is being undertaken to ensure contractors complete the training. **Recommended for closure.**
4	12/11/2020	3.3 Risk, Compliance & Audit Update	**Compliance Update:** Access to Cash: The Committee asked that the draft of the responses to the call for evidence on Access to Cash were circulated to the Group Executive (GE).	Jonathan Hill	ASAP with update to be provided @ January 2021 RCC	30/11/2020: The submitted version was sent by Martin Kearsley to the GE on Thursday 26th November 2020. **Recommended for closure.**
5	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit:** Effectiveness of the Second Line during COVID-19: Ben Foat questioned whether the work being undertaken to put a Controls Framework in place was happening quick enough, noting there had been some delays in getting the project to the Project Review Board. The audit report emphasised that there could not be any more delays. It was agreed that this work should be taken to GE to discuss the need to develop the Framework and the approach that should be taken.	Johan Appel/Ben Foat/Jonathan Hill/CoSec (agenda)	Further update to be provided at March 2021 RCC ~~ASAP with update to be provided @ January 2021 RCC~~	05/01/2021: A update on this work is contained within the Compliance Paper to be presented to the Committee on 12 January 2021. A further update will be provided when further work has been undertaken. 30/11/2020: Rebecca Whibley has flagged to CoSec team for GE agenda. Johann Appel/Jonathan Hill to advise of timing and provide paper. A whole project has been set up to push this forward and actions are already underway on GLO-related matters. A formal project plan is being built in parallel to the activities being done as we have just been getting on with it. Also, a business case is being created for submission in January to cover the whole of Post Office. An update will be provided in January 2021.

POL00423694

6	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit:** Joiners, Movers & Leavers (JML): The Chair stressed the importance of completing this work. The risks for internal movers needed to be mapped and resolved. Lisa Cherry was asked to take this away.	Helen Rhodes & Tony Jowett ~~Lisa Cherry~~	Update to be provided @ March 2021 RCC ~~ASAP with update to be provided @ January 2021 RCC~~	05/01/2021: IT have worked through the leavers and work is continuing on the movers. This work will be compelted prior to the January 2021 ARC meeting. 03/12/2020:This work is being carried out by Tony Jowett and Helen Rhodes.
7	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit**: Further actions were also highlighted as needed to be completed prior to the report being submitted to the ARC: -The addition of Dan Zinner's comment to the Branch Hub (Programme Assurance) summary. -On the outstanding data privacy (document retention) action, it needed to be explained why the 31 October date had not been deliverable and what the new date was. If the issue could not be remedied, there needed to be detail as to what controls would be put in place. This should also be reflected in the Data Governance paper (see paragraph 16).	Johann Appel/Jeff Smyth (second bullet)	November 2020 ARC	30/11/2020: These changes were made to the report which was submitted to the ARC for its meeting in November 2020. A separate paper on the data privacy action was provided to the ARC for noting and it was agreed by the ARC that the management action would be revised in line with the solution that was presented to the ARC. The action due date will be re-set to 31 March 2021. **Recommended for closure.**
8	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit:** Further, it was requested that: Johan Appel send the headline details of the Special Investigation to the Chair.	Johann Appel	ASAP with update to be provided @ January 2021 RCC	30/11/2020: A verbal briefing was provided in confidence to Al Cameron on 19 November. **Recommended for closure.**
9	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit:** Further, it was requested that: Ben Foat and Jeff Smyth discuss offline the rules around deleting/not deleting data for legal reasons.	Ben Foat & Jeff Smyth	Update to be provided @ March 2021 RCC ~~Update to be provided @ January 2021 RCC~~	06/01/2021: Ben and Jeff have met to discuss the rules regarding data preservation in "legal-hold" situations and we have confirmed that there is no automatic deletion of any Outlook Email, Sharepoint or Onedrive based data. Data access is deactivated in employee leaver situations but that data is still retrieval on request by line management or other authorised requestors. Data Protection have recommended that to keep within POL risk appetite that IT, in conjunction with Compliance, need to start working towards an initial purge of the emails systems and the implementation of an auto delete solution when the Legal Hold is removed.
10	12/11/2020	4.2 Cyber Security	**Cyber Security:** It was requested that Tony Jowett provide a list of all individuals who have not done the phishing training to the relevant GE members.	Tony Jowett	Update to be provided @ March 2021 RCC ~~ASAP with update to be provided @ January 2021 RCC~~	05/01/2021: This will be provided to all GE members ahead of ARC paper submission on 18 January 2021.
11	12/11/2020	4.2 Cyber Security	**Cyber Security:** Jeff Smyth and Lisa Cherry also agreed to flag the need for comms with Nick Read and highlight the issue with the Leadership Group.	Lisa Cherry & Jeff Smyth	ASAP with update to be provided @ January 2021 RCC	16/12/2020: This was highlighted to the Leadership Group and mentioned in a 10@10. **Recommended for closure.**
12	12/11/2020	4.2 Cyber Security	**Cyber Security:** Tony Jowett was further asked to update the paper for the ARC reflecting the action that was being taken.	Tony Jowett	November 2020 ARC	30/11/2020: This was included in the paper for the ARC in November 2020. **Recommended for closure.**
13	12/11/2020	4.2 Cyber Security	**Cyber Security:** Tony Jowett also noted that his team were looking at tool to monitor culture shift and it was agreed that he would liaise with HR on the on-going culture work to build this into the business' longer term defence plans.	Tony Jowett	Update to be provided @ March 2021 RCC ~~ASAP with update to be provided @ January 2021 RCC~~	05/01/2021: Initial meeting has been held with Juliet Lang in People team and plans are in development. An update will be provided at the March Committee meeting.
14	12/11/2020	4.3 Joiners, Movers, Leavers	**Joiners, Movers, Leavers:** The highest exposure areas were being prioritised (leavers and movers) due to the recent organisational design work. Lisa Cherry confirmed that all processes for leavers and movers were being reviewed to ensure all bases were covered and Tony Jowett and Helen Rhodes have weekly meetings with further regular touchpoints between the relevant teams. The regular list of leavers shared with IT has been expanded to include those at risk of redundancy such that this could also be monitored proactively. Tony Jowett was asked to put the detail relating to the focus on leavers and movers in the summary section of the paper for the ARC.	Tony Jowett	November 2020 ARC	30/11/2020: This was included in the paper for the ARC in November 2020. **Recommended for closure.**

POL00423694

15	12/11/2020	4.4 Belfast Data Center (Horizon) Disaster Recovery Post Test Briefing	**Belfast Data Center (Horizon) Disaster Recovery Post Test Briefing**: The current plan was to not to do another test of this size and scale this financial year but to ensure that as part of Belfast Exit there was equivalent activity in suitable point i.e. latter point of the next calendar year. The Chair commented that this was one of the business' biggest risks and felt that another test should be done at Easter given the recent test was only partially successful. Jeff Smyth explained that the test was expensive (circa £75,000) and also destroys all change programme activity hosted in the secondary data center. The Chair noted that £75k was a tiny sum compared to the cost and reputational damage of losing branch trading. It was agreed that the GE should agree the timing of the next test.	Gary Walker / CoSec (agenda)	Update to be provided @ March 2021 RCC ~~Update to be provided @ January 2021 RCC~~	06/01/2021: This item is targeted to be presented to the GE for a decision before the end of January 2021. 30/11/2020: Rebecca Whibley has flagged to CoSec team for GE agenda. Gary Walker to advise of timing and provide paper.
16	12/11/2020	5. Suspense of Accounts	**Suspense Accounts:** There was a question around the extent to which the report and its findings could trigger disclosure obligations, although the vast majority of the report was not disclosable. Mark Underwood was requested to ask the GE whether they wished the report to be fully disclosed or a redacted version. (Post meeting note: Mark Underwood has advised that the ARC would be asked to discuss whether the KMPG report should be disclosed at its November 2020 meeting).	Mark Underwood/ CoSec (agenda)	November 2020 ARC	30/11/2020: The ARC was asked to approve disclosure and felt it necessary to refer to the Board. This was therefore discussed and approved by the Board in November 2020. **Recommended for closure.**
17	12/11/2020	6. Notification of Transaction Error	**Notification of Transaction Error:** It was agreed that the outcome of the investigation into the error should be published in the interests of transparency (Tim Perkins to arrange).	Tim Perkins	Update to be provided @ January 2021 RCC	~~17/12/2020~~: 1.Since the last RCC, Post Office has completed an RTQ process and raised a Purchase Order for work to be completed to prevent duplicate auto transaction corrections from being issued in the future. This work will also include a non-related enhancement that will prevent any transaction correction narrative from being cut off after 500 characters. These enhancements will cost £9,860 and are due for completion by 19/03/2021. 2.Once these enhancements are completed, a Branch Focus article will be published to explain the enhancements and to give Postmasters reassurance that when Post Office identifies issues that impact them, it will respond by clearly publicising the issue and making changes that ensure the issue cannot recur. Given the expected completion date for the enhancements, the Branch Focus article should be published in late March 2021. **Recommended for closure.**
18	12/11/2020	8. Agreed Upon Procedures	**Agreed Upon Procedures:** Tom Lee introduced the paper, which had been circulated previously and was taken as read. The Committee challenged the number of findings in the Note Circulation Scheme (NCS) area. Tom explained that the bulk of these related to evidence that was not available due to COVID-19. The remaining issues were not major concerns and had been shared with Bank of England, who were comfortable with the findings. A detailed action plan has been set up and would be fully implemented by the end of the month. Tom Lee was asked to include these points in the executive summary section of the report.	Tom Lee	November 2020 ARC	30/11/2020: This change was made to the paper which was submitted to the November 2020 ARC. **Recommended for closure.**
19	12/11/2020	9. Historical Matters Unit (HMU) Governance Review	**Historical Matters Unit (HMU) Governance Review:** It was explained that much progress had been made to set up the Governance of the new HMU, but it was not yet finalised. It was noted that this should be made clear in the paper to the ARC. Further Ben Foat explained that the HMU would follow the usual business policies and would only have an exemption in terms of litigation. Notably Post Office has not signed up to the Crown Services legal panel so this should be corrected.	Graham Hemmingway	November 2020 ARC	30/11/2020: This change was made to the paper which was submitted to the November 2020 ARC. **Recommended for closure.**

POL00423694

20	12/11/2020	11. Terms of Reference	**Terms of Reference:** The Chair introduced the paper which had been circulated previously and was taken as read. The Committee APPROVED the draft Terms of Reference for onward submission to the GE, subject to the following amendments: -It should be specifically called out that the Committee has oversight of the HMU; and -The membership should be updated to include: Alisdair Cameron, Ben Foat, Jeff Smyth, Lisa Cherry, Amanda Jones and Cathy Mayor.	Rebecca Whibley	December 2020 GE	14/12/2020: These were approved at the December GE meeting and are available on the intranet and in the Diligent Reading Room. **Recommended for closure.**
21	12/11/2020	12. Deepdive: Multiple partner financial stability update	**Deepdive: Multiple partner financial stability update:** Amanda Jones further explained that small retailers had done better than expected during the COVID-19 crisis. However, WH Smiths were having some difficulties but thought they were financially strong and well placed to recover. They have announced 25 high street closures, including six Post Offices. The business was already aware of two of these. There was likely to be some noise around these as they were recent franchises (Amanda Jones was asked to check the legal position regarding WH Smith closing recently franchised branches).	Amanda Jones (delegated to Katie Secretan)	Update to be provided @ January 2021 RCC	06/01/2021: Commercial Partners are faced with the same challenges of all retailers in this current climate, however, we do not have any significant concerns. Reduction in trading hours are being discussed with some CP's but none fall below the minimum/core trading hours. From the 1st January, WHSmith have reduced to core trading hours in 102 of their Post Offices (Monday to Friday 9am to 5:30pm; Saturday 9am to 12:30pm; Sunday closed) to ensure commercial viability, and a PO service offering. Increased hours will be reviewed in line with customer demand. In regard to resignations, CJ Lang (SPAR retailer) resigned on 28 of their PO branches during July/August last year, all but 4 of these will be closed this financial year. This was not driven by Covid, but the non-commercial viability of the PO in these sites. The retail continues to trade, and the PO will be replaced by a Food to Go offering. IRRELEVANT IRRELEVANT IRRELEVANT will close in Q4 (this financial year); 3 in Q1; 1 in Q3 and 1 in Q4 2022. With regard to the specific recourse for the closing branches, it has been confirmed that there is recourse for POL and this being worked through with Legal. **Recommended for closure.**
22	12/11/2020	16. Data Governance	**Data Governance:** The Committee felt that the business needed to be sure that there was no data that was otherwise unknown to the wider business being stored elsewhere. The following points were discussed: -The Committee requested that Procurement check that there are no other contracts for data storage or archiving other than those with the Postal Museum and Oasis.	Barbara Brannon	Update to be provided @ January 2021 RCC	30/11/2020: Procurement have advised that the only providers are Box-It/Oasis & Postal Museum. **Recommended for closure.**
23	12/11/2020	16. Data Governance	**Data Governance:** The Committee felt that the business needed to be sure that there was no data that was otherwise unknown to the wider business being stored elsewhere. The following points were discussed: - An individual needed to be assigned to go into each admin building to check cupboards and rooms to ensure there was no data that was unknown.	Jonathan Hill	Update to be provided @ January 2021 RCC	30/11/2020: The action was set out in the Data paper that was noted by the ARC in November 2020 and is being actioned. An update is provided in the Complinace paper for January 2021. **Recommended for closure.**

POL00423694

24	12/11/2020	16. Data Governance	**Data Governance:** Accordingly, the Legal, Data Protection, IT and Ruk Shah (MI & Analytics Director) were asked to work on a coherent recommendation on how the data retention policy should evolve and how it will be implemented. This should return to the RCC and ARC in January 2021. Further, the current paper needed to articulate the next steps and process that will be worked through.	Ben Foat, Jeff Smyth, Jonathan Hill (delegated to Sarah Gray, Chris Russell)	Update @ March 2021 RCC ~~January 2021 RCC & ARC (paper update for November 2020 ARC)~~	06/01/2021: This is addressed in the Compliance paper to be presented to the Committee on 12 January 2021. Progress is being made and the primary focus is to provide information as required for GLO disclosures on 5 February 2021 (deadline date for disclosure for the 41 past convictions referred for appeal by the CCRC to the Court of Appeal (Criminal Division)). A further update will be provided at the March Committee meeting. 30/11/2020: The Data Governance paper was updated as requested and submitted to the November 2020 ARC for noting.
25	12/11/2020	17. Procurement Governance & Compliance Report	**Procurement Governance & Compliance Report:** Barbara Brannon introduced the paper, which had been circulated previously and was taken as read. The following points were highlighted: -End User Computer Services (EUC): the project was re-baselined and as a result the revised plan targeted April 2021, which was later than the date provided to the Board. The Public Contract Regulations (PCR) risk was unchanged but the exit service risk was higher and IT were looking at the plan. -Common Digital Platform (CDP): The tender process has slipped and at present the application support and development services were unlikely to have been completely retendered or moved to other existing PCR compliant contracts by December as proposed to GE and Board and there were concerns in respect of resourcing and funding. -Smith & Williamson: This contract was just being finalised with Finance and would be submitted to the Board. -Audit Contract: A compliant extension option existed to extend but PWC were currently working at risk preparing an audit plan for 2020/21 while commercial terms are being negotiated. -Cheque Clearing: (Greg Lewis joined for this update only) A risk exception was submitted to Board in June 2020 to extend our cheque clearing services with Barclays IRRELEVANT The service was needed as Post Office has a IRRELEVANT IRRELEVANT IRRELEVANT The recommendation was to complete an RFI before Christmas to understand the market and this would IRRELEVANT to IRRELEVANT The Chair requested that these items should be covered in the paper for the Board, noting that the business needed to be as transparent as	Barbara Brannon	November 2020 ARC/Board	30/11/2020: This paper was prepared for the ARC and was shared offline with Lisa Harrington (only member of the Board who does not attend ARC meetings). **Recommended for closure.**

POL00423694

26	10/09/2020	4. Pensions Assurance	The Committee requested a timetable and proposed quantum ahead of the ARC meeting, but noted that LC was due to meet the Chair of ARC separately to discuss this issue.	Lisa Cherry / Maxine Cross	Update @ March 2021 RCC Meeting ~~Update @ January 2021 RCC Meeting~~ ~~September~~	05/01/2021: The Trustee has now received reconstructed pensionable pay and allowances data. This is being reviewed to assess both the differences to the 2017 data that formed the basis of the Rothesay buy-in and the quantum of the overpayments. A report is expected to be presented to the Trustee Board in March 2021 along with the Trustee rectification plans. The regulator has been updated and is expecting more information from POL at the end of the March. 06/11/2020: Project Assurance Steerco has been created and will be meeting monthly following the initial meeting on 30th October 2020. Initial sets of reconstructed data were shared with the Trustee and Willis Towers Watson, POL's scheme advisors. Both wondered if the scheme rules had ben correctly interpreted which led to legal advisors for both POL and the Trustee reversing an earlier view about the application of the scheme rules. Data is being recalculated in accordance with the later view and is now expected to be completed in mid-November with POLs reviews expected to conclude at the end of November 2020. We intend to notify The Pension Regulator of this delay to the rectification timetable following their acknowledgement of our breach paper. In October, the POL Board was advised of a potential liabilities stemming from a provision in the Pension Administration Agreement. Our legal advisors think that the liabilities under this agreement will be capped at £300k (£150k per "event".)
27	13/07/2020	3.5 Compliance Report	Fairness - the Telco team was asked to consider ways to reduce the number of 'vulnerable customers' and to revert to the Committee with a statement/plan for November.	Jonathan Hill / Meredith Sharples	November RCC & ARC Meeting	23/12/2020: This action is no longer required given the sale of the telco business due in January 2021. **Recommended for closure.** 02/11/2020: This will be included in the Compliance Paper presented to the RCC & ARC. NOTE: there is an error in the minutes and the action should read: *"the Telco team was asked to consider ways to reduce the number of customers out of contract and to revert to the Committee with a statement/plan for November."*
28	07/11/2019	10.6 - Money Laundering Reporting Officer (MLRO) Annual Report	BF, SS and JH talk to retail on enforcing three lines of defence and suggested BF attend a meeting with HMRC.	Sally Smith / Jonathan Hill	Update @ January 2021 RCC Meeting	31/12/2020: The HMRC supervisor who took over when the previous supervisor retired in May 2020 moved to a new role in the summer. A further supervisor was appointed in August 2020 and an initial virtual meeting has been held, but due to continuing Covid restrictions, HMRC are not undertaking any supervisory visits or meetings, and it is unclear when this will recommence in 2021 or what the frequency or format of meetings will be with this new supervisor. **Recommended for closure.** 02/11/2020: HMRC are still conducting any meetings - action to be updated at next meeting (January 2021). 09/07/2020: HMRC are not conducting meetings at present due to Covid, but Sally has chased.

POL00423694

29	07/11/2019	3.2 Supplier Contracts out of Governance	SSK – retail lead team decision required to ensure project does not stall.	Kathryn Sherratt / Nick Wade /Cathy Mayor / Marketing Additional: Angus MacDonald/Barbara Brannon/Lisa Watkins	Update @ March 2021 RCC (resolution by end of January 2021) ~~Update @ January 2021 RCC (resolution by end of January 2021)~~	05/01/2021: Commercial and legal negotiations are ongoing but are on track to complete a compliant support renewal of the legacy SSK estate by January end. 02/11/2020: SSK Procurement Project will now be formally closed and any future activity will sit under the Network Strategy workstream. Automation forms a clear part of this strategy and is fully backed by the Board. Network Strategy is due to go back to Board in January with an update on Automation and Technology (this includes SPM dependencies and route to procure). In relation to the existing estate the procurement team are investigating a PCR compliant route to maintain the current estate and potential procurement of new with a target resolution date of 29/01/2021. Previous: The SSK Procurement Project is on hold at present. This work will now form part of NEO Work Package 5, which is due to report to Board in June and July on Network Shape and Formats and Propositions respectively. NEO WP5 will return to Board in September with the Technology part of the work stream, the direction from which will form part of the Procurement. The project will return to PRB to resume work following the September Board.
30	07/11/2019	3.3 Supplier Contracts out of Governance	Brands/RAPP – Agree date for tender	Jeff Smyth / Marketing (David Enwright) Additional: Barbara Brannon	Update @ January 2021 RCC Meeting (contract by end of November)	23/12/2020: A compliant tender process has been run and the contract has been awarded to the incumbent provider, with operational costs reduced. The contract has been signed and is available on Web3. **Recommended for closure.** 02/11/2020: A compliant tender process has been run and the contract has been awarded to the incumbent provider, with operational costs reduced. Contracts are nearing finalisation with a target completion date of end November.

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

3.1

Title:	Risk Report	**Meeting Date:**	12 January 2021
Author:	Mark Baldock, Head of Risk	**Sponsor:**	Alisdair Cameron, Group Chief Finance Officer

Input Sought: Noting & Approval

The Risk & Compliance Committee (RCC) is asked to note the current status of key risks and GRC implementation and approve draft proposals on the role of the Board and Audit, Risk & Compliance Committee (ARC)/RCC with respect to oversight of Post Office risk management for onward submission to the ARC.

Executive Summary

RCC is asked to

- **note** current progress on the design and build of a GRC tool
- **note** a new set of system supported GRC risk reports will be presented to ARC in 3/2021.
- **note** the key risks we currently face with particular focus on those in the Commercial, Financial, Operational, People and Strategic space
- **approve** draft proposals on how best the roles of the Board and the ARC/RCC with regard to risk management should be clarified, aligned and are mutually supportive

Confidential

POL00423694

3.1

Report

- What are our key risks (new and existing) and their materiality?
- How should our risk profile be governed?

Background

1. In 9/2020 we updated the way in which it reported to RCC/ARC on the status of the Post Office's key risks. We introduced a new Dashboard format designed to not only provide a summary view of the Post Office's overall risk profile but also a bottom up analysis which showed how the lowest level (local) risks related to the next level (intermediate) which, in turn, linked to the highest level (enterprise). At the same time, we began to manage this dataset through RSA Archer. We saw this as a first step in moving the away from a manual (very resource intensive) risk management process to one which would become increasingly automated.

2. Much progress has been made but challenges still remain particularly around our recent inability to rollout out the capability to manage risks to individual business units. Given this, work commenced on the design and build of a Governance, Risk and Compliance (GRC) capability to provide a structured corporate approach to governance, enterprise risk management and regulatory compliance.

3. Phase 1 went live in 1/2021. This involved migrating the Central Risk dataset from RSA Archer to Service Now (IRMPro module). Phase 2 (which is subject to separate approval) will extend this risk management capability team to allow the business to manage their risks via the on-line GRC tool rather than through the Central Risk team. Phase 2 will also involve the migration of the IT and Finance Controls from Traction. This is targeted from the beginning of 2021/22.

4. ARC have welcomed these developments but asked that future risk reports provide a particular focus on the key risks faced by the organisation as well as a summary of the risks across the 3 levels (enterprise, intermediate and local).

5. In doing so RCC are asked to note we have been unable, on this occasion, to provide system-aggregated Dashboards etc as we are just finalising the transition from RSA Archer to ServiceNow (IRMPro). This is scheduled to be completed by the end of 1/2021. A refreshed set of GRC risk reports will be presented to ARC in 3/2021.

6. This paper also provides some thoughts on which types of risks should be discussed at Board and/or ARC.

Key Risks

7. RCC will recall the recently approved Risk Policy places our risks into 14 themes. These are broadly in line with those advocated by HM Government's 'Orange Book'.[1]

8. We consider the key risks we face (new & existing, top-down & bottom-up are primarily in 5 of the 14 themes namely **Commercial**, **Financial**, **Operational**, **People** and **Strategic**. We will now look at each of these in turn. A complete list of our key intermediate risks (rated 12 and above) across all 14 themes is provided as an appendix.

[1] HM Government: Management of Risk – Principles and Concepts (June 2019)

POL00423694

Commercial

9. These are risks associated with the management of commercial partnerships, supply chains and contractual requirements. Failure to manage such risks proactively could mean the Post Office could suffer from poor performance, inefficiency, poor value for money, fraud, and/or fail to meet business requirements/objectives.

10. A key Post Office risk in this area is around the **management of our commercial relationship with Fujitsu** (**4:4**) for the remaining 3 years of the contract. Failure to manage this relationship effectively will not only adversely impact the delivery of the Post Office's Telco strategy but also the timely implementation of Belfast Exit, SPM and PCI compliance. To date, Fujitsu have resisted changes that could adversely impact their financial position or deliver positive change in capability at speed and with control. There is also the possibility Fujitsu may adopt an increasingly defensive commercial position given the ongoing post-GLO Judicial Inquiry.

11. Other commercial partnership risks include IRRELEVANT **the Banks** (**5:4**) IRRELEVANT IRRELEVANT and, of course, IRRELEVANT **with Royal Mail** (**5:3**). IRRELEVANT IRRELEVANT In the event either of these risks materialise Post Office performance service affordability could be undermined which will have a long term adverse impact on the delivery of Post Office's purpose.

12. There are also commercial risks around **adverse trading performance** in part prompted by the ongoing consequences of the pandemic. For example, there is risk that **travel insurance** remains significantly impacted (**4:4**). Although POI have successfully launched a COVID compliant product (and a travel product is back on sale) ongoing and unpredictable European travel restrictions is likely to continue to hamper travel recovery well into 2021. This will impact on POI recovery causing a negative impact on delivering business objectives and/or on commercial viability.

Financial

13. These are risks arising from a **potential inability to managing finances** in accordance with requirements and financial constraints. If such risks materialise the Post Office could see a poor return on investments, a failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

14. At this point the Post Office face a number of risks around **insufficient funding** such as not being provided with sufficient working capital, Network Subsidy, and/or Investment Funding (all of which are currently rated as **4:4**). There are also risks Post Office is not provided with sufficient funding for the Historic Short Scheme compensation (**4:4**) and/or for post-GLO criminal case compensation (**4:4**).

15. In terms of mitigating such risks clearly imminent decisions on working capital facility, Network Subsidy and Investment Funding will allow 2021-22 priorities to be agreed, IRRELEVANT headroom. That said it is also important to note agreed funding levels may result in IRRELEVANT IRRELEVANT IRRELEVANT It is understood a decision on HSS compensation funding is expected in 1/2021. Without funding the HSS scheme will collapse.

Confidential

POL00423694

Operational

16. These are risks that would arise from potentially inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

17. Potentially **ineffective operational delivery** manifests itself as a risk that Post Office is unable to satisfactorily resolve **Agent Postmaster recruitment and retention** at 'Hard to Place' Branches (**4:3**).

18. We also face risks the Post Office fails to deliver an **adequate and attractive remuneration package** for its Agent Postmasters (**5:3**), a material number of **Postmasters are adversely impacted financially because of** IRRELEVANT **(5:3**) and we are unable to effectively manage and secure the **support of Postmaster representatives** (**5:3**).

19. Notwithstanding such risks evidence shows that Postmasters have continued to trade strongly during the ongoing difficult trading conditions (particularly around Mails) and have not reacted strongly to the GLO judgements. It is also the case improvements have been made in the fairness and transparency of processes and improved remuneration.

20. Our sense is that our COVID-19 response (efficient and effective PPE deployment and enhanced remuneration) has been welcomed by Postmasters. Announcements of consultation and Postmaster Board representation have also been well received. Nonetheless, challenges remain including maintaining and enhancing Postmaster earnings, IRRELEVANT IRRELEVANT as well as formalising new contracts and managing representative bodies.

21. Another key operational risk is around the potential **financial fragility of multiple partners (3:3)**. To help mitigate this risk arrangements have been put in place for the regular financial monitoring of large multiple partners to pick up early warning signs. In addition, work continues on the development and delivery of a refreshed network strategy coupled with the delivery of new flexible & attractive propositions (including increased automation).

22. Finally, the Safety Board have recently discussed a potential increased risk of **physical crime by external parties** (**4:3**). This has prompted, in part, by very high levels of cash being deposited at a small number of branches. To mitigate this risk, we are reducing the amount of cash in branches with highest holdings, increasing the number of cash collections at specific locations and introducing security deterrents and protection including body armour and cash destruction (i.e. glue and ink capability).

People

23. These concern risks of potential ineffective leadership and engagement, a sub-optimal business culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

24. In this area Post Office clearly face potential risks around an **inadequate Work-Life balance**. The **pressure on Post Office Central teams** is large and increasing (**4:4**)

POL00423694

and ongoing and protracted home-working arrangements could have an increasingly adverse impact on the well being of Post Office employees (**4:4**). It also apparent the recent Post Office organisational structural changes has increased the risk of **material loss of corporate memory** (**4:4**).

25. In part such risks are a direct consequence of continuing pressure to downsize the organisation to reduce costs and the aim of having a smaller number, more agile workforce supported by increased automation. However, transitioning to such an end-state has significant challenges. The pressures on central teams is large and increasing and is complicated by job uncertainty, the pain of GLO findings and the particular pressures of home working.

26. It is also the case that in the event Post Office does not proactively engage with the CWU there is a risk of **prolonged industrial action (3:4)** which would adversely impact our ability to deliver our short, medium or long-term strategic objectives resulting loss in revenue, client/customer detriment and reputational damage. There is growing concern that some form of industrial action will take place due to the planned reduction of the DMBs. In terms of mitigation a dispute resolution has been put in place (including GOLD teams) and relevant stakeholders have been engaged.

Strategic

27. These concern risks arising from pursuing a strategy which is subsequently seen as poorly defined, and/or is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment.

28. In this context the Post Office, like most companies, is subject to **adverse external economic factors**. There is risk therefore we are unable to react quickly to fluctuations in the economy that increase or decrease demand for our products and services (**4:4**). Clearly at the moment there is greater economic uncertainty than normal due to COVID-19 and Brexit. Indeed, this uncertainty is so widespread that most commercial organisations are re-assessing their operations, viability and approach, which may create an (unforeseen) secondary impact. It is also the case that Government economic policy is stressed and its overall direction is unclear. Economic changes are already and are likely to create both opportunities and risks as markets, competitors and partners change.

Risk Governance

29. The Post Office Risk Policy is clear the organisation's risk governance consists of the:
    - **Board:** They are informed and advised by ARC. The Board have overall accountability for the assessment and management of risk, taking a strategic view of the risks faced by Post Office;
    - **ARC/RCC**: They support the Board in its assessment and management of risks. The ARC reviews Post Office's risk policy, risk appetite and attitude to risk to ensure these are appropriately defined and communicated so that parameters and expectations are understood; and,
    - **Group Executive (GE)**: The GE, led by the Chief Executive, has operational responsibility for Post Office risk management and systems of internal control.

30. This structure is underpinned by a standard '3 lines of defence' risk model whereby the **GE and Post Office Groups** (and their subsidiary business units) perform the 1st line

POL00423694

function, **Central Risk** the 2nd line function and **Internal Audit**, who operate independently of 1st and 2nd Line functions, the 3rd Line.

31. Although the Policy does not prescribe what specific risks should be considered at what level it is clear the relevant governance groups must have the requisite authority for the risks they own/consider and, where not, the risks should be escalated.

32. This suggests, using such broad principles as a guide that the
    - **Board** should oversee
        - the 14 enterprise risks given such risks are, by their very nature, Post Office-wide and so are of strategic importance.
        - any specific intermediate risk which
            - exceeds, or is projected to exceed, its approved appetite
            - impacts multiple business areas
            - requires action by multiple stakeholders
            - requires corporate change to mitigate
            - requires the endorsement of the major stakeholder
        - any other risk formally escalated to it by ARC, RCC or GE

    - **ARC** should
        - provide initial assurance of the Central Risk Board report with particular focus on the status of key risks (by ratings), their trends, trajectory and the extent to which they are being proactively mitigated and are within appetite
        - oversee the operation of the '3 lines of defence' risk model to ensure assurance is aligned
        - oversee the application of the Post Office's risk policy (and supporting risk management framework), the design and implementation of specific risk appetite statements and their supporting KRIs

Next Steps

33. The RCC are asked to
    - **note** current progress on the design and build of a GRC tool
    - **note** a new set of system supported GRC risk reports will be presented to ARC in 3/2021
    - **note** the key risks we face with particular focus on those in the Commercial, Financial, Operational, People and Strategic space
    - **approve** draft proposals on how best the roles of the Board and the ARC/RCC with regard to risk management can be clarified, aligned and become mutually supportive

POL00423694

Appendix: Post Office key risks (12+) by Theme

Risk ID	Risk Theme	Risk Title	Inherent Risk Score	Recent Risk Score
RSK-106	Change	Impact of Post GLO on Change Portfolio	20	12
RSK-45	Change	Strategic alignment of Change Initiatives	12	12
RSK-70	Commercial	Government Services	20	20
RSK-117	Commercial	POI - Travel Insurance Market	16	16
RSK-101	Commercial	POI EBITDAS Recovery	20	16
RSK-69	Commercial	Banking Services dependency	15	15
RSK-68	Commercial	Royal Mail Dependency	15	15
RSK-100	Commercial	POI - Appointed Representative (AR) -POL:	20	12
RSK-120	Commercial	POI - Recessionary pressure .	12	12
RSK-89	Financial	COVID uncertainty hampers strategic decision making	16	16
RSK-64	Financial	Digital income	20	16
RSK-119	Financial	POI - Cashflow	16	16
RSK-44	Financial	Costs due to Group Litigation	12	12
RSK-43	Financial	Insufficient funding	12	12
RSK-107	Health & Safety	Health & Safety breach	20	12
RSK-128	Health & Safety	Pandemic - Covid-19 risk of infection to employees and closure of branches	20	12
RSK-126	Health & Safety	Physical crime by external parties	20	12
RSK-125	Health & Safety	Road Risk including failure to follow Road Safety Guidance	16	12
RSK-48	Marketplace & Brand	Customer Demand	20	20
RSK-118	Operational	POI - Second COVID spike or regional spike	12	12
RSK-35	Operational	Postmaster remuneration	12	12
RSK-55	People	Employment Model	15	12
RSK-57	People	Industrial Action	16	12
RSK-91	People	People COVID 19	16	12
RSK-81	Security	3rd Party Managed Systems Cyber Threat	15	12
RSK-53	Strategy	Telco dependency	20	20
RSK-61	Strategy	Existing Product Simplicity	12	12

Confidential

POL00423694

Risk ID	Risk Theme	Risk Title	Inherent Risk Score	Recent Risk Score
RSK-27	Strategy	Strategic Design	12	12
RSK-75	Technology	Business Continuity and Disaster Recovery	15	12
RSK-73	Technology	Legacy IT Infrastructure	15	12
RSK-63	Technology	Reliance on Third Party Suppliers	15	12

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

3.2

Title:	Corporate Legal & Compliance Risk Appetites: An Assessment	**Meeting Date:**	12 January 2021
Author:	Jonathan Hill, Director of Compliance, Sarah Gray, Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Approval

The Risk & Compliance Committee (RCC) is asked to approve the corporate Legal & Compliance Risk Appetite Statements for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

RCC is asked to **note:**

- the paper applies the previously ARC approved Risk Appetite methodology to the **corporate** perspective of legal & compliance risks across Post Office.

- In doing so, this paper notes the risk appetite of legal and regulatory issues are managed through the three lines of defence compliance model. Generally, the LCG function provides, amongst other things, 2nd line of defence for legal and regulatory risk management. This is not therefore a paper on the risks within the LCG function per se but rather Legal and Compliance risks as they apply across the organisation. So include, for example, the consequences of non-conformance with contractual obligations, statutory requirements, regulatory requirements, corporate compliance (including control effectiveness), and disputes/litigation. Once approved the appetites will **apply to all risks** in this space wherever they sit in the business.

- the risks have been grouped into **6** themes (Contract & Transaction Management Obligations, Statutory & Regulatory requirements, Disputes & Litigation, Employment, Pensions & Associated Disputes, Corporate Compliance & Control Environment and Intellectual Property & Brand). The Disputes & Litigation appetite **excludes** post-GLO activity and Starling which are reported to the Board separately. We consider the attitude to risks around the Historical Shortfalls Scheme merits a specific appetite assessment. This is being pursued.

- work is being finalised on the supporting Key Risk Indicators (KRIs). We have already identified an extensive range, but further work is required to complete the activity. This will be done imminently and, by itself, should not prevent approval of these statements.

DRAFT SUBJECT TO FURTHER COMMENTS

Confidential

POL00423694

ARC is asked to **approve** the Post Office should have

Appetite	General and Specific Risk Categories	Outcome
An **Averse** appetite	to being non-compliant with our **Statutory & Regulatory requirements (excluding PCR)** and **Crimson Employment, Pensions & Associated Disputes**, (noting that we will be adopting a neutral appetite to specific risks around other employee complaints and employment law claims)	If confirmed, we are **within tolerance** at the moment with most of these risks although there are a small number currently outside of tolerance
A **Cautious** appetite	to being non-compliant with risks around our **Compliance and Control environment and PCR in procurement**	The Control Review Project will confirm the extent to which we are **within** tolerance here.
A **Neutral** appetite	to **Contract & Transaction Management Obligations, Disputes & Litigation** (excluding post-GLO) and **Intellectual Property & Brand**	If confirmed, we are **within** tolerance here (except for the risk around workers rights).

We have outlined a series of next steps subject to securing approval.

Report

- What is the Post Office's appetite to corporate Legal & Compliance risks?
- How are our current risks trending against such appetites?
- What are we doing to bring any such risks outside of tolerance within appetite?
- What are our proposed Next Steps and the timeline?

Background

1. In 11/2020 the ARC approved an updated Post Office Risk Policy which outlined an a new approach to **Risk Appetite** such that we can meet our strategic objectives of (i) supporting Post Office Postmasters, (ii) building a fit for purpose network and, (iii) focusing relentlessly on Post Office core strengths and customers.

2. The Policy defines **Risk Appetite** as the amount of overall risk the Post Office is willing to pursue (or retain) to achieve its strategic objectives. It also outlines a new 5-tiered appetite scale (ranging from '**Averse**' which borders on zero tolerance, through '**Neutral**' to '**Open**') against which individual risks will be assessed. In doing so the Policy requires several factors to be considered including (i) our **tolerance for uncertainty** ((ii) our **decision choices** and (ii) our **strategic priorities.**

3. The approved Risk Appetite scale is provided at **Appendix A**. Since approval we have **include some indicative risk rating ranges** as a guide. These can be adjusted.

4. The General Counsel's view is that the strict wording and definitions of Appendix A (albeit a synthesis of generic industry-wide models) are on the more conservative or cautious side of the classifications when benched-marked to other specific companies. Depending on the Board's review of the application of Appendix A scale to the Legal & Compliance risk appetite statements and assessment, it may choose to revise the scale. For the purposes of this paper it has been adopted.

Legal & Compliance Appetite

5. In parallel with Central Risk updating the Risk Policy and establishing a supporting corporate approach to risk appetite the business has looked at how we can proactively apply these tools and techniques to the corporate legal and compliance risks.

6. We have the grouped the **26** individual corporate Legal & Compliance intermediate risks, which are set out in Appendix B, into **6** themes (Contract & Transaction

DRAFT SUBJECT TO FURTHER COMMENTS

Confidential

POL00423694

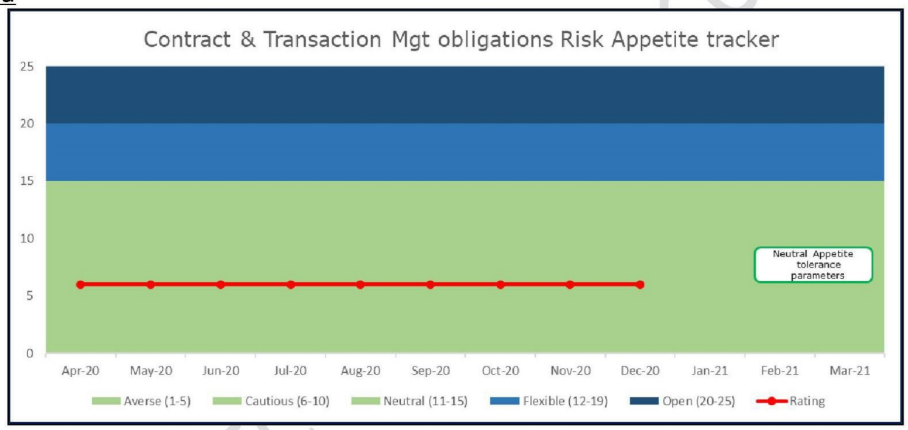
Management Obligations, Statutory & Regulatory requirements, Disputes & Litigation, Employment, Pensions & Associated Disputes, Corporate Compliance & Control Environment and Intellectual Property & Brand). We have scoped the **Disputes & Litigation appetite to exclude post-GLO activity and Starling**. This is for a number of reasons including the need to differentiate between our attitude to risks around the Historical Shortfalls Scheme with those relating to other litigation. The former will be subject to a separate appetite assessment.

7. The **26** risks and their current risk ratings are provided at **Appendix B**.

8. The **6** themes are described in turn in the remainder of this paper. Each provides a tailored description of our attitude to the risks in that area, how the current risks trend against this and what we have in train to bring any within tolerance where it is necessary to do so.

Contract & Transaction Management Obligations

Risk Trend



Commentary

9. We have a **Neutral** appetite to being non-compliant with our contract and transaction management obligations. This means, on balance, we will accept risks could materialise here but only if their adverse impact is limited and are heavily outweighed by the benefits. Active risks in this area **will target a combined average impact and likelihood risk rating of between 1-15.**

10. At the moment we have **one** intermediate risk. This is around the potential failure to manage our contractual obligations resulting in a **risk of not realising assets and commercial value** (i.e. from the benefits under the contract (**3:2**).

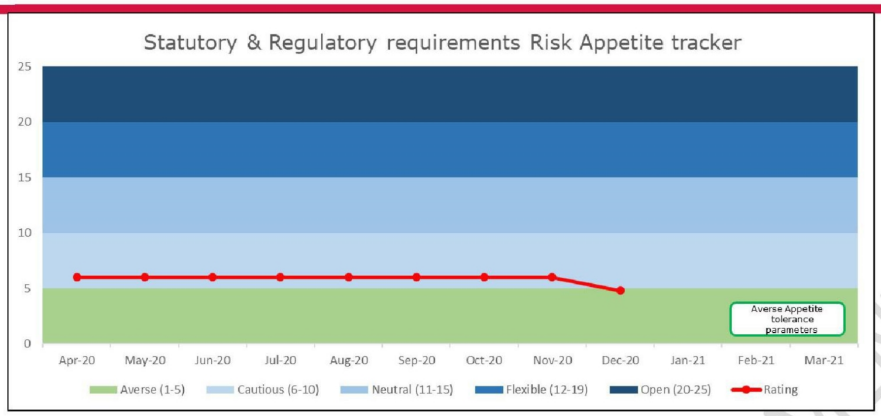
11. This risk is **in line with a Neutral appetite**. so can be simply tolerated but monitored. No further mitigations are required.

Statutory & Regulatory requirements

Risk Trend

DRAFT SUBJECT TO COMMENTS

POL00423694



DRAFT SUBJECT TO FURTHER COMMENTS

Commentary

12. Across this theme, in most circumstances, we broadly have an **Averse** appetite to being non-compliant with our statutory and regulatory obligations (other than PCR). So, we will avoid taking pretty much any risk in this area (where at all possible) and have an extremely low appetite for any new risks materialising. In line with such an appetite any active risks we manage **will target a combined average impact and likelihood risk rating of between 1 and 5**.

13. Given the sectors in which we operate it is not surprising we have a significant number of statutory and regulatory obligations, a number of which have associated risks identified against them. These include potential **non-compliance with new and emerging regulation**, an **inability to meet evolving FS regulatory requirements**, **adverse regulatory investigation**, **anti-money laundering non-compliance**, **anti-bribery & corruption non-compliance**, **data protection non-compliance** and **inadequate management of Whistleblowing incidents**.

14. The majority of these risks have a risk rating of 5 or below which means they are **in line with an Averse appetite** (but sometimes on the cusp) so no further mitigations are required and they can be tolerated. However those risks on the outer limit of tolerance will be carefully monitored to ensure they do not breach appetite.

15. **Two** risks (with an averse appetite) are currently breaching tolerance. These are
    - Adverse regulatory investigation: if the Post Office engages in anti-competitive behaviour, there is a risk that regulators or competitors could investigate and successfully challenge such behaviour resulting in regulatory sanctions, penalties, financial and reputational damage. This risk has a current rating of (**5:2**). We consider this rating is merited given the high impact if Post Office engage in this type of behaviour (e.g. fine of up to 10% turnover, third party damages, actions, reputational damage etc). Mitigation measures are currently being worked on by Legal to bring within risk appetite. This includes competition compliance training being provided to Payzone and Legal teams from November 2020.

    - Anti-Money Laundering non-compliance: If the Post Office fails to maintain AML processes, policies and training there is a risk that it becomes non-compliant with the requirements of anti-money laundering regulations. This risk has a current rating of (**3:2**) so is just exceeding an averse tolerance. This score has been reached primarily due to the risks associated with Fit & Proper, Premises

POL00423694

Registration and Sanctions data anomalies. For example in the last 12 months, there have been instances of fit and proper data integrity issues, a small number of deregistered branches being able to transact Travel Money and ongoing issues with the current AML Credence Universe pulling through customer data on potential Sanction matches.

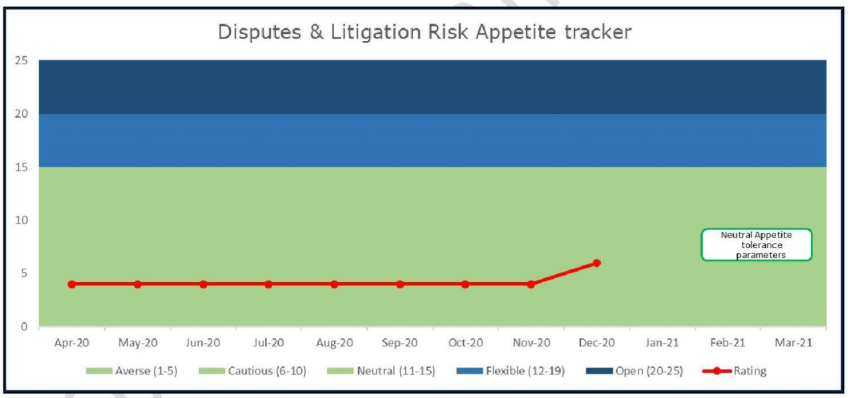
There are control remediation actions in place to improve the control strength and effectiveness in this area thereby reducing the residual risk scope once secured. These are covered in more detail in the MLRO Report.

16. It should also be noted we have a statutory and regulatory risk with a **Cautious Appetite**. This concerns the risk of **non-compliance with Public Procurement Rules** (PCR) which has a rating of (**3:2**) so is well within tolerance so can be simply tolerated. We consider a cautious stance is appropriate here given the Board have approved a PREN process which allows the approval (in limited instances) of direct awards and PCR non-compliance.

17. That said the Procurement and Legal teams are working closely with the business to increase PCR compliance and mandatory PCR compliance training has been rolled out across the business from December 2020.

Disputes and Litigation

Risk Trend



Commentary

18. We have a **Neutral** appetite to risks around Disputes and Litigation (excluding GLO and Starling). This means, on balance, we will accept risks could materialise here but only if their adverse impact is limited and are heavily outweighed by the benefits. Active risks **will target a combined average impact and likelihood risk rating of between 1-15**.

19. We only have **one** intermediate risk in this area around **Upstream clients and suppliers being successful in litigation and disputes** (**3:2**)

20. This risk is currently assessed as **in line with a Neutral appetite** so can be simply tolerated but also monitored.

21. As we have mentioned elsewhere this specific theme excludes GLO and Starling. The latter will be picked up by the Historical Shortfall scheme. However ARC will wish to be

Confidential

POL00423694

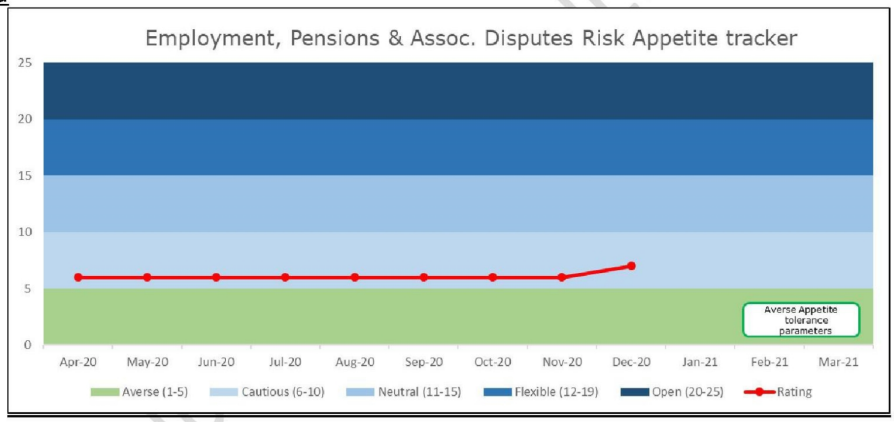
aware we have articulated a specific risk around Starling which is privileged and subject to separate reporting.

22 [redacted]

23. We note the Starling litigation is due to be heard in June. [redacted]

Employment, Pensions and Associated Disputes

Risk Trend



Commentary

24. As with our statutory and regulatory obligations we have an **Averse** appetite to risks around failing to comply with "crimson" statutory or regulatory requirements in the employment and pensions space. So, we will avoid taking pretty much any risk in this area (where at all possible) and have an extremely low appetite for any new risks materialising. In line with such an appetite any active risks we manage **will target a combined average impact and likelihood risk rating of between 1 and 5**.

25. We have **two** intermediate risks here. One is around the risk of the Post Office being **non-compliant with 'crimson' statutory and regulatory requirements, relating to employment and pensions law**. This risk is rated as (**2:2**) so is within appetite.

26. The other is around the risk of being **non-compliant with other employment and pensions law obligations** which could result in employee complaints, claims, industrial action, or regulatory fines. Although we assess this risk as (**5:2**) on this topic we consider we should have a greater flexibility here and therefore adopt a cautious

Confidential

POL00423694

rather than an averse stance. This brings this specific risk within tolerance of the former.

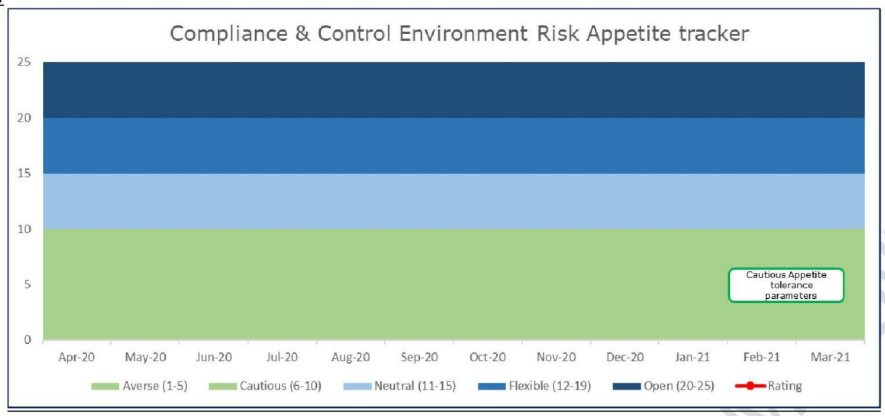
DRAFT, SUBJECT TO FURTHER COMMENTS

Confidential

POL00423694

Compliance & Control Environment

Risk Trend



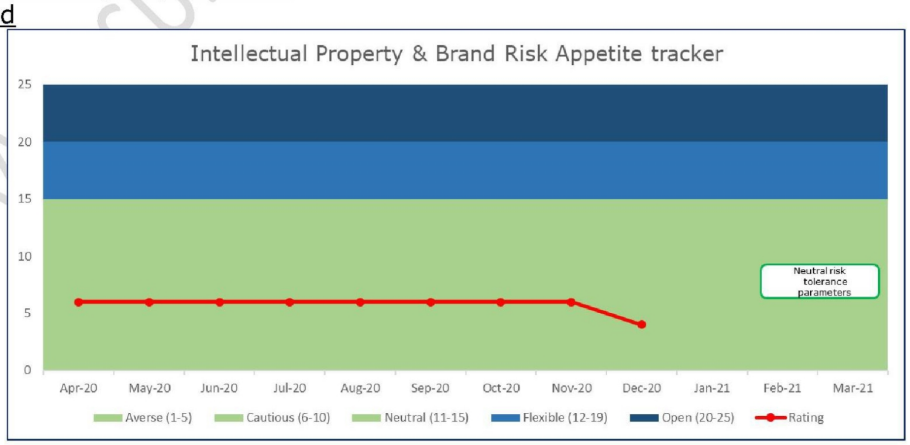
Commentary

27. We have a **Cautious** appetite to risks around our Compliance and Control environment. So, although we will take a conservative approach to such risks, we also acknowledge some could materialise. However, this will only be acceptable to us if the activity giving rise to the risk is essential and the possibility and extent of failure limited. Any active risks **will target a combined <u>average</u> impact and likelihood risk rating of between 1-10.**

28. At this point we have identified **three** very similar intermediate risks in this area, albeit with different causes namely (i) failing to have appropriate and effective controls in place, (ii) failing to follow or comply with the controls that are in place and (iii) a lack of clearly assigned accountabilities. Any of these causes are seen to give a similar risk of **non-compliance with Post Office's legal and regulatory requirements**. At the time of writing the Control Review project is focused on clarifying the detail of these associated risks (and their impact and likelihood) in parallel with the analysis of the effectiveness of the associated controls. A Cautious appetite will be applied once the ratings are confirmed

Intellectual Property & Brand

Risk Trend



Confidential

POL00423694

Commentary

29. We have a **Neutral** appetite to being non-compliant with our contract and transaction management obligations. This means, on balance, we will accept risks could materialise here but only if their adverse impact is limited and are heavily outweighed by the benefits. **Active risks will target a combined average impact and likelihood risk rating of between 1-15**.

30. We have **one** active intermedate risk around **third parties misusing the Post Office brand and trademark** which could result to customer confusion and detriment (**2:2**). This risk is currently assessed as **in line with a Neutral appetite** so can be tolerated but monitored. No further mitigations are required.

Next Steps

31. The ARC are asked to **approve** that we should have
    - an **Averse** appetite to risk of being **non-compliant with our Statutory & Regulatory requirements (excluding PCR)** and **Employment, Pensions & Associated Disputes**, (noting that we will be less averse to specific risks around employee complaints and employment law claims)
    - a **Cautious** appetite to risks around our **Compliance and Control environment and PCR in Procurement**
    - a **Neutral** appetite to **Contract & Transaction Management Obligations**, **Disputes & Litigation**, and **Intellectual Property & Brand**)

32. The ARC are asked to **approve** that when viewed collectively the risk ratings within each group are broadly in line with their associated appetite. There are a small number of individual risks breaching tolerance which need to be managed accordingly and a small number whose appetite has been flexed slightly, some of which are outside tolerance.

33. The ARC are also asked to **note** that subject to approval we will ensure the target risk ratings are fully aligned with the associated appetite. We are also finalising work on the associated KRIs. We have already identified an extensive range and this work will be completed imminently. This does not prevent approval of the appetites.

34. We will require risk owners of any corporate legal & compliance risk outside of appetite (and wherever owned in the business) to proactively manage them to bring them within tolerance.

35. Central Risk will provide assurance on such activity and will include an assessment of risks against their approved Risk Appetite (along with the latest KRI trends) as part of the bi-monthly RCC/ARC reporting.

DRAFT, SUBJECT TO FURTHER COMMENTS

Confidential

POL00423694

Appendix A: Post Office Risk Appetite scale (ARC approved)

	Appetite rating	Impact/Likelihood Rating span	Risk taking philosophy	Tolerance for Uncertainty[1]	Decision choice[2]	Prioritisation of Strategic Objective[3]
↑	**Open**	**21-25**	Will take risks and **accept the possibility of failure**	Will **accept the possibility of failure**	Will choose the **option with the highest return**	**Will accept risks could materialise** and the achievement of (some) strategic objectives could be compromised
	Flexible	**16-20**	Will **take justified risks**	Will choose the option which has **some degree of risk**	Will accept risks materialising subject to being **able to proactively manage their adverse impact**	**Will accept (under certain conditions) risks could materialise** the achievement of (some) strategic objectives could be compromised
	Neutral	**11-15**	**Prefers, on balance, safe delivery to risk taking**	Will **accept, on balance, risks** could materialise	Will accept risks could materialise but only if **adverse impact is limited and heavily outweighed by benefits**	Would **prefer ideally not to accept** risks materialising if this meant the achievement of (some) strategic objectives could be compromised
	Cautious	**6-10**	Will take a **conservative approach to risks**	Will **accept some risks** could materialise	Will accept some risks materialising but only if activity is essential and the **possibility and extent of failure is limited**	Would be **somewhat reluctant** to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised
	Averse	**1-5**	Will **avoid nearly all risks** where at all possible	Has an **extremely low appetite for any risks** to materialise	Will always select the option with the **lowest risk**	Would be **extremely reluctant** to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised

[1] **Tolerance for uncertainty**: How willing is Post Office to accept uncertain outcomes? This illustrates the Board's appetite to trade off certainty to achieve a given objective. A low rating demonstrates the Board's need for certain outcomes, while a high rating shows the Board will pursue an objective even with an uncertain outcome.

[2] **Decision choice**: When faced with multiple decision options, how is Post Office willing to select a decision that puts a strategic objective at risk? This question assesses the Board's acceptance that a given choice may lead to failure to meet a strategic objective. A Board who are averse will only choose options that pose a minimal threat to the strategic objective's achievement. A Board open to this risk are willing to trade off the possibility of failure for a high-risk, high-reward decision.

[3] **Prioritisation of strategic objective**: How willing is Post Office willing to trade off this specific objective against achievement of other objectives? This demonstrates the Board's willingness to pursue achievement of a given strategic objective over achievement of another. A Board who are averse to this would never trade off completing the objective in question for failure of other objectives. A Board which is open would be willing to accept this trade-off.

Confidential

DRAFT, SUBJECT TO CONTRACT

POL00423694

Appendix B: Legal & Compliance Intermediate Risks – Inherent and Current Ratings

Risk Title	Risk Description	Residual Score	Appetite	Comment
Contract and Transaction Management Obligations				
Post Office fails to realise the commercial value of its assets	If Post Office fails to manage its contractual obligations, there is a risk that it will not realise its assets and commercial value (i.e. from the benefits under the contract)	**6**	Neutral	This is a commercial/financial risk flowing from contractual rights/obligations. Impact unlikely to exceed £5m. Measures such as Contract Management Framework and training to contract managers mitigate risk.
Statutory & Regulatory Requirements				
Post Office non-compliance with Public Procurement Rules	If the Post Office fails to comply with Public Procurement Rules, there is a risk the most appropriate suppliers are not selected and/or the Post Office could suffer financial and reputational damage (e.g. a successful legal claim from an aggrieved potential supplier could result in award of damage, a fine, contract being set aside etc)	**6**	Cautious	PCR compliance risk appetite has shifted in 2020 from averse to cautious, with the Board implementing the PREN process to approve limited instances of direct awards and PCR non-compliance. Accordingly, some compliance risk is accepted. As mitigation, Procurement and Legal teams work closely with the business to drive PCR compliance and mandatory PCR compliance training has been rolled out across the business in December 2020.
Post Office non-compliant with new and emerging regulation	If Post Office fails to identify and implement new and emerging regulation, there is a risk that Post Office would breach its statutory and regulatory obligations resulting in regulatory sanction, penalties, financial and reputational damage	**3**	Averse	Inherent risk is impact 3 could be reportable to regulators and likelihood 3 possible. Residual impact score remains the same, but likelihood reduced to remote 1. Rationale for residual score: We have a number of controls in place to manage this risk, these include the Law and Trends Forums, the horizon scanning activities by all 3 Principals as well as that undertaken by the FS Compliance team. The Banking framework partners via SCGC also highlight new requirements. The remote risk would be for all of these requirements to be wilfully ignored.
Post Office operating model non-compliant with new regulation	If new additional regulation is imposed on Post Office and it fails to modify its operating model, there is a risk that it will be less able to compete effectively and efficiently resulting in declining revenue and margins.	**6**	Neutral	This is a commercial risk that LCG have insight into, and it may also be appropriate to be evaluated outside of LRG. Inherent impact assessment could be up to £5m and the likelihood is 'possible' so 9 scored for inherent risk. The residual score of 6 is based on the impact remaining at 3 and the likelihood of 2 unlikely. Rationale for residual score: The future regulatory changes include ; 'Access to Cash', where HMT have already consulted on them appointing a new regulator. This will include regulations for the cash infrastructure that could include PO . We also have pending Link membership where industry obligations will need to be assessed and met. However, the net likelihood assessment of 2 is based on these changes being actively managed to help support the changes.
Financial Services FCA/FS non-compliance	There is a risk that the Post Office fails to comply with the requirements of FCA and the Financial Services regulations.	**4**	Averse	Inherent score is impact 3 could be reportable to regulators and likelihood 3. Rationale for residual score: Compliance overall is currently in a good place as measured in dashboard and reports to Principals (excluding travel insurance) so the impact is moderate, and likelihood is 'unlikely but could occur' seems appropriate- Residual score 4

DRAFT, SUBJECT TO FURTHER COMMENTS

Confidential

POL00423694

Risk Title	Risk Description	Residual Score	Appetite	Comment
Post Office non-compliance with 'crimson' statutory and regulatory requirements	There is a risk that Post Office fails to comply with the "crimson" statutory and regulatory requirements (e.g. licence to trade or those with severe sanctions e.g. criminal liability). If this risk materialises Post Office could suffer catastrophic financial loss, reputational damage, regulatory sanctions and penalties	**3**	Averse	Only covers DP, FS and AML Inherent risk is impact 3 could be reportable to regulators and likelihood 3 possible. Residual impact score remains the same, but likelihood reduced to remote 1. Rationale for residual score: We have a number of controls in place to manage this risk, these include the Law and Trends Forums, the horizon scanning activities by all 3 Principals as well as that undertaken by the FS Compliance team. The Banking framework partners via SCGC also highlight new requirements. The remote risk would be for all of these requirements to be wilfully ignored.
Adverse regulatory investigation	If Post Office engages in anti-competitive behaviour, there is a risk that regulators or competitors could investigate and successfully challenge such behaviour resulting in regulatory sanctions, penalties, financial and reputational damage	**10**	Averse	Potential impact is high if POL engages in this behaviour (e.g. fine of up to 10% turnover, damages claim etc). Mitigation measures are being worked on by Legal to bring within risk appetite - competition compliance training has been provided to PZ and Legal teams in Nov 2020.
Customer detriment and Upstream client Contract breach	If Post Office fails to comply with financial services regulation, there is a risk of customer detriment, breach of contract with upstream clients including Appointed Representative Agreements, leading to financial and reputational damage	**3**	Averse	Inherent risk is impact 3 could be reportable to regulators and likelihood 3 possible. Residual impact score remains the same, but likelihood reduced to remote 1. Rationale for residual score: We have a number of controls in place to manage this risk, these include the Law and Trends Forums, the horizon scanning activities by all 3 Principals as well as that undertaken by the FS Compliance team. The Banking framework partners via SCGC also highlight new requirements. The remote risk would be for all of these requirements to be wilfully ignored.
FCC Anti-Money Laundering Anti-Money Laundering non-compliance	If Post Office fails to maintain AML processes, policies and training there is a risk that it becomes non-compliant with the requirements of anti-money laundering regulations and is subject to fines, sanctions and reputational damage.	**6**	Averse	There are 18 local risks that make up this intermediate risk, 10 of which are scored between 6 – 8 (Amber). This intermediate risk is scored as a 6 primarily due to the risks associated with Fit & Proper, Premises Registration and Sanctions data anomalies. In the last 12 months, there have been incidents where • There are on-going F&P data integrity issues. Resulting on one occasion in requesting HMRC approval of a late submission of monthly data. • In October, it was identified that 6 deregistered branches were able to transact Travel Money. Historic inconsistencies were subsequently identified and showed 35 branch records were in accurate relating to Travel Money. This failing was reported to HMRC, who confirmed that they would be taking no further action or sanction against POL but confirmed that they will judge all matters on their individual circumstances and therefore any repeated breaches may result in sanctions. • There continues to be issues with the current AML Credence Universe pulling through customer data on potential Sanction matches. After review, it was confirmed that none of the customers were Sanctioned individuals. There are control remediation actions in place to improve the control strength and effectiveness. The above is also covered in more detail in the MLRO Report.
FCC - Anti-Bribery & Corruption: Anti-Bribery & Corruption non-compliance	If Post Office fails to maintain ABC processes, policies and training there is a risk that Post Office employees and/or its Postmasters engage in bribery or corruption, resulting in potential fines, sanctions and reputational damage	**4**	Averse	There are 3 local risks that make up this intermediate risk, which relate to the training, ABC policy and Gifts & Hospitality tool. The controls are assessed as effective, with exception being training, where recent resource changes have impacted the delivery.
FCC Whistleblowing: Inadequate management of Whistleblowing incidents	If Post Office fails to comply with Whistleblowing requirements, there is a risk that reported concerns will not be properly investigated and or unethical or illegal behaviour would not	**2**	Averse	

DRAFT, SUBJECT TO FURTHER COMMENTS

Confidential

POL00423694

POST OFFICE

Risk Title	Risk Description	Residual Score	Appetite	Comment
	be identified, and could lead to regulatory sanctions and penalties, and financial and reputational damages			
FCC Financial Crime	If Post Office fails to maintain Financial Crime processes, policies, training there is a risk that Post Office fails to prevent and detect financial crime resulting in potential fines (by regulator or Card Scheme), sanctions and reputational damage.	**4**	Averse	There are 10 local risks that make up this intermediate risk, 4 risks shared with AML intermediate risk. These local risks include the Financial Crime policy, resource, Dynamics case management system, card fraud report monitoring
Data Protection: Data Protection non-compliance	As a result of an organisational or technical failing there is a risk that Post Office does not comply with data protection legislation and is subject to fines and/or sanctions and reputational damage through non-compliance its policy and controls. The impact of this would be a lack of confidence from Customers and partners such as Government and Banking Services partners.	**4**	Averse	The inherent risk was taken Pre-GDPR programme and was scored as a 3-5. Given all the remediation work that we have put in place and the controls adopted that our Corporate risk should be scored as 4-1. The impact has gone up as the fines post-GDPR are more severe
FCC Supply Chain Compliance Supply Chain non-compliance	If Post Office fails to maintain controls (i.e. policies and processes) in relation to supply chain compliance there is risk that Post Office fails to comply with regulatory requirements and is subject to potential fines, sanctions and reputational damage	**3**	Averse	There are 3 local risks that make up this intermediate risk, which relate to resource and the team's capability to carry out regulatory responsibilities. The controls are assessed as effective therefore reducing the likelihood.
Disputes & Litigation				
Upstream clients and suppliers successful in litigation and disputes	If Post Office fails to manage its contractual obligations, there is risk of litigation & disputes with its upstream clients and suppliers resulting in financial and reputational damage	**6**	Neutral	Comments against RSK-[xx] apply here. GLO and Starling are not included and have a significantly higher risk profile
NEW [privileged and subject to separate reporting] Successful Postmaster challenges on 'worker rights'	[redacted]			
Employment, Pensions and associated disputes				
Post Office non-compliance with 'crimson' statutory and regulatory requirements, relating to employment and pensions law.	If Post Office fails to comply with the "crimson" statutory and regulatory requirements (i.e. failing to pay National Minimum Wage or other statutory minimum employment payments, knowingly employing Illegal workers, committing Modern Slavery Act or related offences, failing to make appropriate and timely reports to, or obstructing the investigations of, a Regulator, or breaching other statutory or regulatory requirements that give rise to severe sanctions e.g. criminal liability), there is a risk that Post Office could suffer significant financial loss, reputational damage, regulatory sanctions and penalties	**4**	Averse	
Employee complaints, Employment & Pension Law claims and complaints to regulators.	If Post Office fails to ensure that its other employment and pensions law obligations (arising from contract, statute, regulation, common law or otherwise) are not complied with there is a risk that Post Office may receive employee complaints, employment law claims, industrial action, or regulatory fines resulting in financial and reputational damage.	**10**	Neutral	
Corporate Compliance & Control Environment				
Post Office breach legal and regulatory requirements (1)	If Post Office fails to have appropriate and effective controls (or such controls are not fit for purpose, there is a risk that legal and regulatory obligations will be breached resulting in regulatory sanction, penalties, financial and reputational damage	**Tbc**	Cautious except Crimson obligation	The Control Review project is focused on clarifying the associated risks (and their impact and likelihood) in parallel with the analysis of the effectiveness of the associated controls
Post Office breach legal and regulatory requirements (2)	If the Post Office business fails to follow or comply with its controls, there is a risk that legal and regulatory obligations will be breached resulting in regulatory sanction, penalties, financial and reputational damage	**Tbc**	Cautious except Crimson obligation	The Control Review project is focused on clarifying the associated risks (and their impact and likelihood) in parallel with the analysis of the effectiveness of the associated controls
Post Office non-compliant with legal and regulatory requirements	If there is a lack of clearly assigned accountabilities, there is a risk of non-compliance with Post Office's legal and regulatory requirements resulting in regulatory sanction, penalties, financial and reputational damage	**Tbc**	Cautious except Crimson obligation	The Control Review project is focused on clarifying the associated risks (and their impact and likelihood) in parallel with the analysis of the effectiveness of the associated controls
Intellectual Property & Brand				

POL00423694

Risk Title	Risk Description	Residual Score	Appetite	Comment
Third party misuse of Post Office Brand & Trademark	If the Post Office fails to enforce its legal and IP rights there is a risk that third parties could misuse the Post Office brand and trademark which could result to customer confusion and detriment as well as financial and reputational damage {neutral / flexible}	4	Neutral	

DRAFT, SUBJECT TO FURTHER COMMENTS

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

3.3

Title:	Compliance and Audit Report	**Meeting Date:**	12 January 2021
Author:	Jonathan Hill, Director, Compliance Johann Appel, Head of Internal Audit	**Sponsor:**	Al Cameron, Group Chief Finance Officer Ben Foat, Group General Counsel

Input Sought: Noting & Decision

The Committee is asked to:

1. note the Compliance update, in particular:
   - The Controls Framework update;
   - The Data Management activities;
   - Post Office's approach to cookies;

2. approve the Data Governance recommendation to establish a Post Office-wide Data Governance framework and SteerCo, based on the Digital Data Governance framework but extended to encompass all forms of data;

3. approve the recommendation to assess the impact on Post Office's approach to cookies of new European regulatory rulings against Google and Amazon, which may result in changes to our cookie management and impact the business; and

4. note the Internal Audit update, specifically progress being made with delivery of the Internal Audit programme and completion of audit actions.

for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

This paper provides an update on key and emerging risks, compliance matters and an update on the latest internal audit position.

Confidential

POL00423694

Compliance

Controls Framework

1. The Controls Framework project has been established, initially, to review/identify gaps in the controls established for the activities done to address the Group Litigation Order (GLO) matters. We are working with the Historical Matters Unit (HMU) project teams, who are identifying processes that have been updated or need updating following the Common Issues judgement (CIJ), Horizon Issues judgement (HIJ) and the establishment of the Stamps Scheme.
2. An interim report is expected before Christmas from KPMG relating to the HIJ, which the Controls project will use as the basis to conduct controls reviews of the Horizon issues.
3. Plans are being developed with the HMU to review the actions taken to address the Stamps issues, starting in January, which will include reviewing the associated controls.
4. Ways of working have been agreed between both HMU CIJ and Controls project teams ensuring clarity of responsibilities and areas of focus. Weekly working group sessions are in place to review progress to date, update on actions and make decisions.

Progress to date:

5. Recruitment of Controls Compliance Analysts.
6. The HMU team is mapping the processes and controls for Transaction Corrections, these are being reviewed by the Control Framework analysts.
7. Changes to around 70% of processes have been made to the Onboarding of new Postmasters, the Controls Framework project team is reviewing these to understand what controls are in place and how effective they are
8. Designing and building a temporary Workflow on 'Power Apps' Tool to record controls information against each business process, and facilitate assessment, assurance and MI for the Controls Framework project
9. Testing the workflow tool and producing a training pack for the business outlining how control owners and operators will need to support the project
10. Drafting a controls assurance template to support and facilitate the control assurance work, ensuring design and operating effectiveness and consistency of Controls work;
11. A work plan for the Stamps Scheme and Controls review is being developed, with the review planned for January and aiming to complete in February 2021, subject to Covid restrictions.

Key issues:

12. There are various lists of actions taken to address the CIJ findings (e.g., the Norton Rose Fulbright ("NRF") review) but we are waiting on the HMU's CIJ project pan to ensure we have one, consolidated approach. In the meantime, activities are aligned to the NRF review list of actions.
13. Initial controls reviews have identified that there is no consistent approach to mapping the processes, if any, for activities addressing the CIJ remediation actions, which makes it difficult to for the business to identify its controls and the project to provide assurance that the controls exist and are effective.

Remediation activities:

14. In the absence of a consolidated list we are using the NRF review as the basis of our controls review workstream
15. Where process maps are missing we are working with the HMU CIJ team to support the creation of process maps
16. This may lead to re-work to assess the robustness of controls, where additional activities are identified at a later date

Confidential

POL00423694

Next steps:

17. Framework workstream:
    - Design business-wide controls framework (draft early January 2021)
18. Controls system
    - Define the user requirements for a permanent controls system (draft early January 2021)
19. CIJ controls review
    - Continue review against NRF list (timeline dependent on findings for each activity)
    - Refresh work plan following updated activity project plan from HMU team
20. HIJ controls review
    - Develop workplan following receipt of KPMG's HIJ interim review (early January 2021)
21. Stamps review
    - Conduct assurance review of Stamps Scheme actions, including associated controls (January-February 2021), aligning with HMU team
22. Business case
    - Develop business case for funding beyond Prove Plan for resource for CIJ, HIJ and Stamps Scheme, plus roll out of Controls Framework and Controls Framework system across all Post Office activities and functions

Telecoms

Sale

At the time of writing, the telecoms sale is due to complete in January 2021. A number of questions are still be addressed by the transaction team. These include:

- Management of historical and post-sale complaints relating to pre-sale matters.
- The continuing of a PSD2 audit for premium rates calls, scheduled for January 2021.
- Existing Ofcom information requests that are due in Q4 2020/21.

23. Ofcom has not yet been informed of the final decision but we have advised the Telecoms team this should be done ahead of signature.

Comms incident

24. We are due to send Ofcom a letter to inform them that all inbound comms and outbound comms have been addressed to put the customer back into the circumstances they would have been if there had not been a communication failure. We are waiting to hear if Ofcom will investigate.

Annual Best Tariff Notifications

25. Annual Best Tariff reminders have started being sent and are planned to be completed by 14th February 2021 in line with the regulation. We expect complaints to rise as customers will ask why they have been paying higher out of contract prices. Customers who have not been subject to a fixed commitment period will receive a bill message, Ofcom may consider that we should be more direct.

Voice only customers

26. Ofcom has released the consultation on its approach to the voice only market, if Post Office were to remain in the telecoms business this would have a material impact on our ability to compete. Given the potential sale, Post Office is not responding to the consultation.
27. The Telco regulatory developments are highlighted at Appendix 1.

Confidential

POL00423694

Data Protection

Data Management

28. Increasingly management of data, in all formats, is a critical matter for all businesses. Data governance in Post Office is managed through a number of different controls and accountabilities. This is a decentralised approach and there is no single record depository that enables the business to quickly identify and manage the data it holds.
29. Although there are a number of controls at the enterprise, group and function level (which are set out through various policies e.g. Cyber & Information Security, Document Retention & Disposal Policy, Protecting Personal Data etc), these are not well understood, nor routinely adhered to.
30. It is recommended that regular monitoring and reporting against these controls through the Risk & Compliance Committee (RCC) and ARC is required if Post Office is to successfully embed them within its operations and manage its data. To enable this, it is recommended that Post Office expands the remit of the Digital Data Governance framework and associated SteerCo to cover all data, including physical documents and data stored in external systems as well as the processes and procedures for managing it, with one accountable member of Group Executive (GE).

Legal Review of "31,000" Boxes for Starling and Criminal Cases Review Commission (CCRC)

Starling:

31 [redacted]

32

33

34

35

36

CCRC, PCDE and HSS

37. The 4 November Historical Matters Steering Committee approved the recommended actions with these to be undertaken on an expedited basis, having regard to the 5 February 2021 deadline date for disclosure for the 41 past convictions referred for appeal by the CCRC to the Court of Appeal (Criminal Division).
38. Peters & Peters (P&P) has now applied, in conjunction with Herbert Smith Freehills (HSF), case specific and non-case specific search terms to the indices to identify material that may be relevant to the PCDE. The searches resulted a number of records (files or boxes) that have been categorised as either

POL00423694

- Potentially relevant records (e.g. because the descriptions are vague but they contain relevant words, or they are relevant but the date is outside the relevant review period)
- relevant to the PCDE and malicious prosecution workstream based on the descriptions in the indexes.
- Records that are not relevant

39. The 10 December Historical Matters Decision Forum approved a recommendation from P&P to
    - Request all of the clearly relevant records for physical checking
    - Complete a sample of the potentially relevant records. This review is nearing completion and relevant documents were identified in c10% of the boxes sampled. P&P are considering if more records need to be checked. The relevant records identified included
        - case specific material relevant to an individual prosecuted by Post Office Limited (POL)
        - documents where an acquitted individual raised issues with Horizon
        - documents relating to issues identified during the roll-out of Horizon, or shortly before
        - prepared statements for interview
40. The wider "dip sample" exercise of a statistically representative random group of indexed and unindexed boxes (c.100 of each) is being progressed by HSF.
41. The records that form the sample have been retrieved. The scanning was initially delayed due document quality but it is now progressing.
42. In parallel, the HSF case handlers have been trained, enabling the reviews to start w/c 7 December. The sampling is due to complete w/c 25 January.
43. The outcome of the reviews will be reviewed throughout the sampling exercise to give early indication of any potential follow up action. The initial feedback indicates that a significant proportion of the records are receipts. Work is in progress to understand the potential relevance of receipts to the PCDE and HSS activity

Back office sites record assurance review:

44. The RCC instructed Compliance and Legal to instigate a search of all Post Office back office locations to give assurances that all relevant information has been presented to Counsel for Starling and PCDE purposes.
45. 93 locations were initially identified as being in scope.
    - 44 were de-scoped as they have been determined to be 'vacant'
    - Vacant premises had to be cleared of all materials including records.
46. Of the 49 remaining locations the following can be reported:
    - 33 sites confirmed there are no records or information stored onsite
    - 13 confirmed that there are some boxes / files onsite. The highest volume is at the 'corporate sites' in particular Chesterfield and Swindon stock centre
    - 3 are still outstanding, though are expected to be cleared by the time of the RCC.
47. The key challenges are:
    - Determining if records located are relevant considering the broad scope of the legal requirements (HSS, Starling, PCDE, Malicious Prosecutions etc)
    - The mechanism for retrieval and scanning if required. We know from the Oasis exercise that there is limited capacity to scan documents in a timely manner
48. Compliance and Legal are working on the next steps to ensure that all relevant documentation is with external Counsel in time to meet 5th February disclosure timeframes. Next steps include:

POL00423694

- Complete further analysis of the potentially relevant boxes / files using criteria agreed with both internal and external Legal. Focus to be on any with potential PCDE relevance. Target 8th January 2021.
- Develop a proposal for the retrieval and assessment of any of the boxes / files
- Draft a closure report to summarise the findings

Record retention

49. The RCC Data Management paper identified that Post Office businesses needed to give assurances that Record Retention Schedules, agreed as part of the Record Retention Programme, were accurate and covered all processing activities.
50. All Data Owners were identified and provided with a copy of the Retention Schedules, Remediation Logs and copies of the Document Retention and Disposal and Protecting Personal Data policies.
51. Data Owners have expressed concerns with regards to the implementation of the Remediation requirements. The key barriers reported back so far have been lack of resource to implement the changes and the timeframes set for remediation to be complete.
52. The responses from the data owners are being recorded and consolidated by the Chief Information Security Officer (CISO) team as the owner of the record retention policy and compliance is supporting the team. Going forward this should be coordinated through the Data Governance framework.

Record management in branches

53. Compliance, Property Services and the Network team have stood up a mini-project to implement a change programme for Records Management with the Branches. This project will look to:
    - Identify and communicate out to Branches what information needs to be archived and preserved
    - Create a new process for record archiving on a regular basis and not just on the closure of a branch as is the process today
    - Arrange for the necessary materials to be provided to branches to allow for archiving to occur, including boxes, archive content labels and deletion dates
    - Mechanisms for transferring boxes of records from branches to off-site storage facilities.
54. The key challenges will be ensuring that;
    - this project is sufficiently resourced to allow the new processes to be implemented,
    - New processes are developed and shared with relevant stakeholders for consultation
    - Communications and training materials created and shared across the Network to enable a smooth transition into Business as Usual.
55. This work will commence in early 2021 as resources are currently focussed delivering Christmas in branches and on the searches of back office locations.

<u>Post Office Ltd approach to Cookies</u>:

56. The CNIL (French Data Protection regulator) levied significant fines of €100m and €35m respectively against Google (US parent organisation and Ireland subsidiary) and Amazon Europe for breaching French Data Protection legislation with regards to their use of website cookies under the ePrivacy directive. The ruling is not applicable in the UK. However, the ICO is likely take into consideration the finding of the CNIL.
    - Google – CNIL were clear that cookies are only lawful if informed consent has been given. Consent should be requested using a banner on the user's first site visit with a clear link to how cookies can be disabled or opposed. Ability to refuse should be offered in whole and part with information disaggregated by purpose. CNIL imposed

POL00423694

a deadline of 3 months to ensure individuals were adequately informed otherwise a further penalty of €100k would be imposed for each day of delay.

57. Post Office continues to be 'middle of the pack. We believe the Google ruling may have an indirect bearing on our approach to cookies. In order to be compliant, it is recommended that the following actions are undertaken.
    - The Digital team and Compliance to carry out an assessment of the ruling and the implications for Post Office and report back to the next RCC. The changes could include:
    - Default settings for all cookies except necessary to be switched to 'off' in preference centre
    - Persistent bookmark on all pages of Post Office website to allow users to re-access the preference centre at any time
    - Detailed information provided through cookie policy on vendors and duration

General Data Protection Regulation (GDPR) Contract Remediation

58. The Contract Remediation project was formally closed at the end of July as reported to the previous RCC. Work is ongoing on and the number of outstanding contracts remains at 7.
59. On all outstanding contracts GDPR clauses have been agreed by both parties and in two (NCR and Santander) the eCAF process is progressing (the other parties are going internal governance).
60. Fujitsu have agreed all GDPR clauses. The only outstanding issue is with one processing schedule, which requires Legal to agree a position on. We are awaiting a response from Fujitsu Telecoms on agreement with the GDPR contract; it is aware of the significance and are being chased for updates on progress
61. Monthly Contract Review Group meetings continue to monitor progress and support negotiations. This will continue until all outstanding contracts are finalised.

Financial Crime

Compliance with Money Laundering Regulations

62. See separate annual Money Laundering Reporting Officer (MRLO) report.

Anti-Bribery and Corruption ("ABC") update

63. Overall completion of the annual ABC training was 98.4% as at 15th December 2020. The business unit previously at 81.7%, is now at 92.4% completion rate and Learning & Development are liaising with HR Business Partners to identify better controls for contractors.
64. Submissions on the gifts and hospitality tool remain low due to Covid restrictions, however a reminder was issued to colleagues in November due to a potential increase in gifts leading up to Christmas.

Whistleblowing Update

65. All reports received in the last two months relate to the branch network, with the majority received from agent assistants raising concerns about Postmasters and unethical behaviour or conduct. Two reports received relating to a Postmaster subsequently uncovered potential mails fraud that is estimated to be in the region of £500k. This is currently being investigated by Post Office Security Operations, supported by the Royal Mail Investigations team.
66. The contract to procure Protect (UK Whistleblowing Charity) to enable us to undertake self-assessment and benchmarking is nearing completion and this should commence in January. Protect have been asked to deliver tailored training for GE and Senior Managers as early as possible in 2021 and we are awaiting their proposals.

POL00423694

Fit & Proper update

67. Please see the separate annual MLRO report.

External Threats

68. Please see the separate annual MLRO report.

Supply Chain Compliance

69. Remote audit of Supply Chain is progressing, and an interim update has been provided to Supply Chain outlining seven key findings identified to date, to enable them to commence mitigation. Some potential issues have been highlighted relating to outstanding actions in respect of fire risk assessments undertaken in June and July which are currently being investigated by the Head of Health & Safety. It is anticipated the audit will conclude by the end of December.

Financial Services

Multi Principal Review of 1st line controls.

70. Our three regulatory principals, Capital One, Bank of Ireland (BoI) and Post Office Management Services Limited (POMS), are reviewing mystery shopping, training, the risk management framework, quality of sales oversight and internal governance as part of their oversight of the Post Office.
71. The discovery work has recently completed and whilst there will be areas of improvement highlighted, there do not appear to be any material issues raised that would cause the Principals to alter their selling/introducing regulated activity with the Post Office.
72. Whilst we are supportive of this review there a number of items in a 'statement of facts' document that need to be clarified before a draft report is produced.
73. We expect the final report to be produced late January and we will share any key findings with this Committee.

Compliance Monitoring

74. Mystery shopping was suspended until after the peak Christmas trading period. Due to the current uncertainties over regional lockdowns and Tier 4 we will need to review if and how we resume mystery shopping in the new calendar year based on risk.
75. Whilst sales of Travel Insurance in branch are expected to be very low; all of our other financial services products remain on sale and promotional activity is planned for both protection and savings business. For example, throughout 2020 and during both lockdowns Post Office typically was selling c500 savings accounts a week.
76. We will work with Network management our Principals and the mystery shopping company to agree a way forward that balances regulatory risk with the social distancing health and safety risk in in Post Offices.

FS Key Regulatory updates

77. A summary slide of the key future developments is included in the reading room at Appendix 2.
78. Post Office responded to the Her Majesty's Treasury (HMT) call for evidence on Access to Cash in November, which sets out the government's aims for protecting access to cash throughout the UK. Post Office outlined the well-established and increasingly important role it plays in access to cash.
79. As part of this consultation the government is considering imposing a single regulator to have responsibility for a well-functioning cash retail distribution network. We await the government response (no date has been given for this) but we will need to understand any potential regulatory risks or implications for Post Office if is decided that the cash infrastructure should be regulated.

POL00423694

80. The Financial Conduct Authority (FCA) has withdrawn its proposal to establish a single easy access savings rate for all savings account of over one year. This is welcome as it could have caused significant challenges for the future pricing of savings back books and the need to change systems with our partner BoI.
81. The Overall Compliance Dashboards (Appendices 3 and 4) are included in the reading room.

Confidential

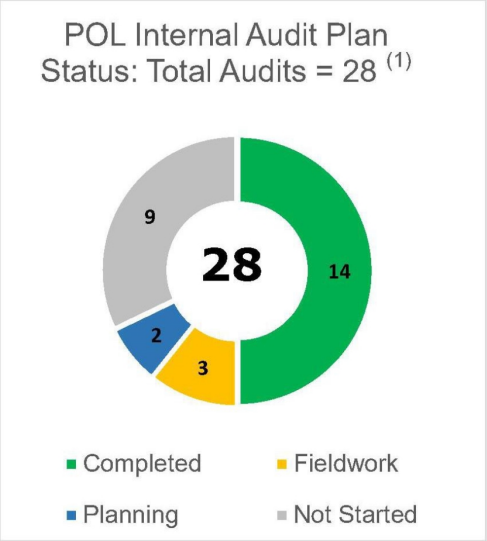
POL00423694

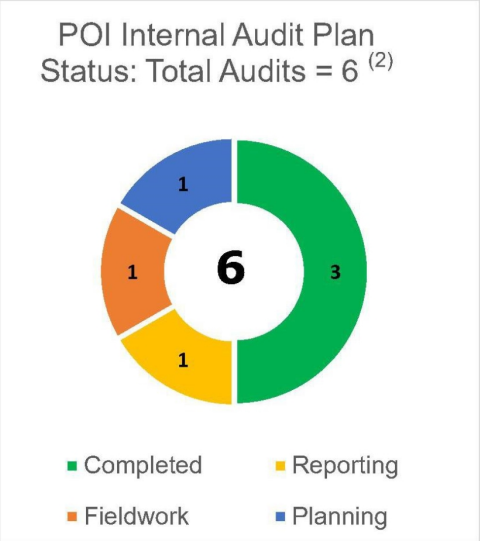
Internal Audit

Progress against Internal Audit plan

82. Delivery of the 2020/21 programme is making good progress, with a further five audits completed since the November ARC meeting (4 POL & 1 Post Office Insurance (POI)). In addition we have also issued one interim report on the Historic Matters CIJ Improvement Programme.

83. Current delivery status is as follows:





(1)Target number of reviews based on revised plan for 2020/21 approved by ARC (18 Internal control reviews & 10 change assurance reviews). Details of the audit plan status are included in the reading room (Appendix 10).

(2)POI ARC approved baseline plan for 2020/21.

84. A re-prioritised Internal Audit programme was approved at the May ARC meeting in response to Covid-19. A more dynamic (quarterly rolling) audit plan was adopted and is being reviewed at each ARC. Further revisions to the plan was approved at the September ARC meeting and is included in the reading room (Appendix 10).

85. The following audits are planned for delivery in Q4:

	Review	Sponsor	Timing	Status
1	Historic Matters (Post GLO) Set-up and Governance	Declan Salter	Oct	Fieldwork (Interim Report Issued)
2	Historic Matters - CIJ Operations Improvement Programme	Declan Salter	Nov	Fieldwork (Interim Report Issued)
3	Postmaster Reporting (MI, Branch Trading Statements)	Amanda Jones	Jan	Fieldwork
4	Postmaster Remuneration (3rd Party Data)	Amanda Jones	Feb	Planning
5	Historic Matters - HIJ Operations Improvement Programme	Declan Salter	Feb	Not Started
6	GLO Historical Shortfall Scheme – Claims & Payments	Declan Salter	Mar	Not Started
7	Third Party Revenue Data Assurance	Al Cameron	Feb	Planning
8	Change Controls Effectiveness	Dan Zinner	Feb	Not Started

POL00423694

9	Strategic Platform Modernisation	Jeff Smyth	Mar	Not Started

Internal Audit reviews completed

86. The following POL audits were completed since the November ARC meeting:

1	IT Control Framework	
2	Mails & Parcels	
3	Historic Matters – CIJ Operations Improvement Programme (Interim)	

4	Belfast Exit Follow-up (Programme Assurance) (Final Draft Report)	
5	PCI Compliance (Programme Assurance) (Final Draft Report)	

87. Our findings and observations from these reports are summarised below (par. 88-92), with the full reports available in the reading room (appendices 5-9).

88. **IT Control Framework** (Ref.2020/21-13)



Sponsor:
Jeff Smyth

Audit actions:

P1	0
P2	5
P3	2
Total	7

Appendix 5

The purpose of the audit was to assess how effectively the IT Control Framework (ITCF) supports IT control assurance and risk mitigation for POL, and whether it reflects the operation of IT related controls across the business and provides accurate and timely information on control performance.

We believe that the approach to implementing the ITCF is sound, based on alignment with an internationally recognised governance framework, with quarterly self-assessment and monthly reporting of status and remediations. The 268 controls that make up the ITCF and are largely aligned with what's happening on the ground and the self-assessment process was generally operating effectively.

Additional work is required to ensure that the ITCF fully supports the business. This should be addressed through migration to a more comprehensive risk and control management tool, and the introduction of strong second line activity to independently validate the self-assessment process.

We conclude that the ITCF has continued to mature since its implementation in 2018 and has further improved since our previous review in 2019. However, we highlight that the operation of the ITCF is not yet fully embedded within the business and was impacted by the absence of a key staff member during April to July 2020.

Management Comment provided by Tony Jowett (CISO)

"Our IT controls framework allows us to better mitigate risks impacting POL's IT. We have reached a very good basic standard of maturity against COBIT 5 and other controls frameworks. This report comes at a perfect time to help us move to the next level of controls maturity. I accept the findings in it and will work to address them. Many thanks for the input."

POL00423694

89. **Mails & Parcels** (Ref.2020/21-16)



Needs Improvement

Sponsor:
Owen Woodley

Audit actions:

P1	1
P2	4
P3	0
Total	5

Appendix 6

The Mails & Parcels business is of key strategic importance to Post Office, contributing one third of PO's total revenue (approximately £350m) in FY20. In Q3 FY21 Mails & Parcels contributed 63% of all Network income.

The purpose of this audit was to review both the Customer and Postmaster journeys for Mails and Parcels products, and to assess the controls in place over related financial, operational and compliance processes.

We found that Post Office are maintaining a positive and effective relationship with Royal Mail Group (RMG), having just successfully negotiated and signed a new IRRELEVANT agreement (MDA2). However, the audit highlighted several issues concerning IRRELEVANT

IRRELEVANT

Management Comment provided by Tom Wasilewski (Head of Commercial Development)

"Given the growing importance of Mails to both the Post Office and our Postmasters a thorough review and audit of its key processes is crucial. The areas highlighted for improvement are right focusing on important drivers of safety and financial performance, and it is satisfying, given the recent signing of the new agreement with RM, that no issues were identified in how that relationship is managed. Compliance and enforcement of Prohibited and Restricted Items (Dangerous Goods) is critical to delivering the high levels of mails integrity our customers expect and the downward trend is concerning making an urgent focus on improvement a priority. However, given the multiplicity of causes and the scale of the network, it is a challenge for which the Mails team will need support from colleagues across the business and we look forward to working closely with them in turning this around. The improving trend in segregation is encouraging and the new contractual arrangements under MDA2 make achieving the new target across all areas a priority".

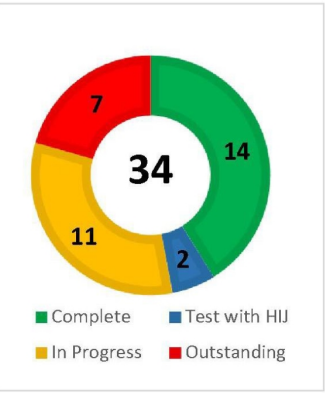
Confidential

POL00423694

90. Historic Matters – CIJ Operations Improvement Programme (Interim Report) (Ref.2020/21-15)

Not Rated *(Interim Report)*

Progress with completion of NRF recommendations:



Sponsor:
Declan Salter

Management comments and audit actions will be in the final report.

Appendix 7

Following the judgments from the Group Litigation Order, Post Office has undertaken a programme of improvements to overhaul culture, practices and procedures throughout every part of the business. In addition to launching the Historical Shortfall and Stamps Schemes, as part of its operational improvement plan, and to address issues which arose from group litigation concluded last year, Post Office has established a new Historic Matters business unit (HM) to oversee and deliver the programme of improvements.

Internal Audit is performing a review of the management and oversight of the improvements delivery, as well as, the appropriateness and sustainability of plans to address the Common Issues Judgment (CIJ) and Horizon Issues Judgment (HIJ) findings. This is being done in three phases.

This second phase of the audit work assessed the programme of measures that will oversee the delivery of the operational improvements to address the criticisms from the CIJ. Primarily, we sought to gain assurance that the operational improvements recommended by Norton Rose Fullbright (NRF), as a result of their analysis of the judgment, have been identified and implemented in accordance with the planned timescales.

We concluded that considerable work has been done to address the judgment findings and implement the 34 NRF recommendations. The status of completion of the recommendations at the time of the audit report, is shown in the chart to the left.

Progress is well evidenced throughout, although in some instances, we have noted differences between the project's view of progress, compared to that of Operations. There is an opportunity to address this by the adoption of a formal handover process that clearly assigns the acceptance of amended documents and procedures by BAU operations.

We highlight that further activity will be required within the business to absorb the impact of the recent OE and the premature departure of some key senior colleagues.

Confidential

POL00423694

91. **Belfast Exit Follow-up (Programme Assurance)** (Ref.2020/21-11)



Needs Improvement

Sponsor:
Jeff Smyth

Audit actions:

P1	0
P2	3
P3	4
Total	7

Appendix 8

Belfast Exit, also known as 'Pivot 2 Cloud', aims to migrate Horizon - the combined group of applications that supports the Retail business of Post Office - from the Belfast data centres (managed by Fujitsu) onto a new cloud platform. The programme was last assessed by IA as part of the 2018/19 plan, with a follow-up review agreed as part of Internal Audit's approved 2020/21 plan.

The objective of this follow-up review was to gain assurance that the revised programme set-up, governance and delivery processes are fit for purpose and operating effectively to enable the envisioned benefits of migrating to the cloud.

Since its restart, the programme has focused on ways to reduce complexity, add scale and delivery throughput, seeking opportunities to add contingency and reduce delivery risks. However, despite the good work done by the team, the technical challenges and the risk of in-flight delays remain significant, as is the potential future cost of failing to address some of the technical challenges faced (technical debt), in order to focus on optimising delivery.

We have rated the programme delivery as Needs Improvement, however, we highlight that **there is a significant residual risk that is outside of the control of the programme**. This risk relates to the fixed deadline of exiting the datacentre when the current lease expires. Management is currently assessing contingency arrangements, with the most likely scenario being a lease extension at an approximate additional cost of £4m. As a result, benefits originally forecasted for FY22 and FY23 may not be achieved.

Management Comment

TBC

Confidential

POL00423694

92. **PCI Compliance (Programme Assurance)** (Ref.2020/21-17)



Needs Improvement

Sponsor:
Jeff Smyth

Audit actions:

P1	0
P2	2
P3	1
Total	3

Appendix 9

The PCI compliance programme is a key compliance risk mitigation programme for Post Office with a high level of risk, complexity and cost. The implications and the level of changes needed to processes and systems supporting both Payment and Banking Services, have led to multiple programme iterations with several business case revisions.

The programme was last assessed by Internal Audit as part of the 2019/20 plan and a follow-up review agreed as part of Internal Audit's 2020/21 plan. The objective of this follow-up review was to gain assurance that the revised programme set-up, governance and delivery processes are fit for purpose and operating effectively.

Significant improvements have been made to the programme since the 2019/20 assessment. In addition, the degree of confidence over the programme's ability to deliver has increased, with the programme highlighting its underlying assumptions and risks in the recent funding submission.

Despite the good work done, key challenges remain in the delivery of a PCI compliant environment. This is primarily a consequence of the inherent complexity of the chosen solutions, which are partly bespoke and the heavy reliance on third parties.

There is a risk of additional costs and further delays in completing the programme, which is not completely within Post Office control, as the current delivery approach is governed by a Time and Materials (T&M) contract with Fujitsu (with Ingenico operating as a subcontractor of Fujitsu).

We note that the programme is still facing challenges in the level of transparency and ease of engagement at functional level with Fujitsu and Ingenico.

Management Comment

TBC

Confidential

POL00423694

Post Office Insurance (POI) Audit Programme

93. The table below shows the status of the POI audit programme:

	Review	Timing	Status
1	Cyber Security (POL-POI Gap Analysis)	Aug	Complete
2	Incident and Breach Management	Aug	Reporting [N1]
3	Data Governance: Ethics, security and privacy • Phase 1 – Third Party Data Security • Phase 2 – Data Governance	 Sept Dec	 Complete Fieldwork
4	Special Investigation (Confidential)	Sept	Complete
5	Pricing: Principles, policies and process	Nov	Complete
6	Effectiveness of Risk Management – original plan	Q4	Planning
7	Channel review: Non-branch sales – original plan	Q4	Not started

[N1] This audit was delayed due to special investigations undertaken at management request and with POI ARC approval.

Status of Audit Actions

94. During May 2020 we agreed with management to provide extended completion dates for 14 actions impacted by Covid-19. All 14 actions have now been completed.

95. The movement and ageing of audit actions are shown in the table below (status at 04 January 2021).

Audit Action Status (POL):	
Open actions at last ARC	29
Less: Actions closed in period	14
Add: New actions in period	24
Total open actions	**39**

Ageing:	
Open (not yet due)	34
Overdue (<60 days)	5
Overdue (>60 days)	0
Total open actions	**39**

96. Following is a summary of the overdue actions and latest status update:

Description of audit finding and Priority rating	GE owner and due date	Action Owners and Status Update
Vetting and Fit & Proper		
Finding (P2): The Vetting Policy is out of date and does not reflect working practices. Action: The Operations Director, Network Operations, will update and re-issue the Vetting Policy, reflecting vetting activity carried out across the business.	Owen Woodley Original date: 31/08/2020 Revised date: 30/11/2020	**Owner:** Tim Perkins (Prev. Julie Thomas) Policy has been updated and is currently with Legal for review, before it will be submitted to RCC for approval. Action expected to be closed before January ARC.
Finding (P2): There is no requirement to confirm qualifications and professional membership or for re-vetting. Action: The Operations Director, Network Operations, in partnership with HR	Owen Woodley Original date: 31/08/2020 Revised date: 30/11/2020	**Owner:** Tim Perkins (Prev. Julie Thomas) Policy has been updated and is currently with Legal for review, before it will be submitted to RCC for approval. Action expected to be closed before January ARC.

POL00423694

will assess whether current vetting practices (including checking of professional qualifications) adequately address the risk of inappropriate or unqualified staff working for Post Office. Any change in approach should be reflected in the Vetting Policy and/or relevant HR Policy.		
Investment Funding Controls - Follow-up		
Finding (P2): Processes and control weaknesses in Anaplan's programme hierarchy. Action: Implement a formal change control process over the hierarchy matrix.	Al Cameron Original date: 30/06/2020 Revised date: 31/12/2020	**Owner:** Max Jacobi MI & Analytics team currently conducting testing on the new reporting capabilities which should be available to the Strategic Planning & Analysis team for month-end reporting. Completion expected before ARC.
Cyber Maturity Assessment 2020		
Finding (P2): There is no concise list of crown jewels agreed with the business. Action: Agree the list of Crown Jewels with POL's GE.	Jeff Smyth Original date: 30/09/2020 Revised date: 30/11/2020	**Owner:** Tony Jowett The list of crown jewels have been updated, but is yet to be agreed by the CIO with the rest of the GE.
Health & Safety Response to Covid-19		
Finding (P2): No formal collation and review of home working assessments undertaken. Action: The Health and Safety team will work with HR to ensure that the appropriate assessments have been completed for all affected colleagues and the necessary actions taken to ensure safe working practices whilst working at home and, where appropriate, e.g. following an Occupational Health assessment adjustments supported and implemented.	Al Cameron Original date: 31/10/2020 Revised date: 31/12/2020	**Owner:** Martin Hopcroft This was due to be rolled out before Christmas with Lisa's wellbeing message to all employees. However, GE directed that the process be delayed until after the busy Christmas period. The message will now be rolled out via GE PA's to all direct reports (for each GE) w/c 4/1/21 and confirmation provided back to H&S team who will then manage interventions as necessary. Expected to be completed before ARC.

Confidential

POL00423694

3.3

Appendices[1]

Compliance

Appendix 1: Telecoms Regulatory Calendar
Appendix 2: FS Regulatory Calendar
Appendix 3: Compliance Dashboard summary
Appendix 4: Compliance Dashboard

Internal Audit

Appendix 5: Internal Audit Report – IT Control Framework
Appendix 6: Internal Audit Report – Mails & Parcels
Appendix 7: Internal Audit Report – Historic Matters – CIJ Improvement Programme
Appendix 8: Internal Audit Report – Belfast Exit Follow-up (Programme Assurance)
Appendix 9: Internal Audit Report – PCI Compliance (Programme Assurance)
Appendix 10: Internal Audit Plan for 2020/21

[1] Appendices are accessible in the Diligent Reading Room.

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	PCI DSS Compliance	**Meeting Date:**	2h January 2021
Author:	Joseph Moussalli, PCI DSS Programme Manager	**Sponsor:**	Jeff Smyth, Group Chief Information Officer

4.1

Input Sought: Noting

The Committee is asked to note:

- What progress has been made during the last reporting period?
- What are the key risks?

Previous Governance Oversight

The Risk & Compliance Committee (RCC) has requested a rolling update on PCI-DSS programme progress.

Executive Summary

The PCI programme has made good progress in several key technical areas, with various milestone having been completed. However, at the time of submission there are two main areas for concern that the programme team is working through. The first is a recent discussion with Santander around their delivery dates which may impact the programme timescales. The second is an ongoing concern around risks associated with programme costs.

The programme consists of 2 core delivery streams:

1. The Point-to-Point Encryption (P2PE) workstream, which encrypts retail and banking transactions from the Pin Entry Device (PED) to a PCI compliant zone in Ingenico before onward processing to Global Payments (retail transactions) or VocaLink (banking transactions).
2. The Target Operating Model (TOM) workstream which addresses use of PCI data by POL in processes outside of the transactions occurring at the PED.

Retail Payments Pilot: During the last period we have implemented the new Ingenico Retail Payments solution in five branches as a limited scale pilot. We are successfully taking Retail payments and settling these transactions with Global Payments. This pilot was delayed by three weeks due to a late defect identified by Fujitsu and caution from Post Office operations due to an unrelated P1 counter issue that was happening at the same time. However, overall, the team has delivered a release of good quality. Initial feedback from the trial is positive, feedback is being collected and this will be factored into the Payment and Banking release.

Banking development: Significant progress has been made by Ingenico in respect of its readiness for Vocalink accreditation, Ingenico has started testing with Vocalink and they remain on track for 21 January 2021. However, the Pilot for Retail Payment and Banking transactions has been impacted due to the significant effort to bring the Retail Payments Pilot (above) into readiness. Fujitsu is indicating a three-week impact to the Pilot readiness date which is now targeted at 26 March 2021 (5 Mar 2021).

Confidential

POL00423694

The Target Operating Model workstream is progressing well and has progressed the secure solution needed for the Financial Crime team and a solution to workaround the Ingenico product limitations of processing BIN ranges greater than 6 digits. There are still some unknown costs – Santander Development, Fujitsu clean-up scripts for the audit.

IRRELEVANT risk

IRRELEVANT were due to migrate their systems to the banking framework by IRRELEVANT. However, mid-December, we were notified by IRRELEVANT that they may not be able to deliver until IRRELEVANT This is despite several escalations through the year about their lack of engagement and Post Office concerns about the delivery timescales. A director level meeting is now scheduled on IRRELEVANT to discuss the delivery forecast from IRRELEVANT and to discuss options to improve on the date. The programme will update RCC following completion of these discussions.

Risk of further Costs

In May 2020, the POL Board approved funding of IRRELEVANT. As part of this Business Case IRRELEVANT of risk was highlighted due to cost uncertainties. Since this approval the programme team has worked to identify and obtain quotations for the work required. We know now that there are IRRELEVANT of confirmed costs but there are still some cost uncertainties which are estimated at IRRELEVANT

The programme is in the process of requesting incremental funding at GE, IC and Board in January 2021. Given the two risks above the programme team requires more time to better the required cost envelope and as such we will only seek approval for the costs to support the programme to March 2021. The programme will then return to board in March 2021 with more certainty about the risks and the costs.

POL00423694

Questions addressed

1. What has been the progress since the programme last presented in May 2020?
2. What are the key risks and issues on the programme?

Report

1. What has been the progress since the programme last presented in November 2020?

Summary of key achievements in the last period:

- IT workstream:
  - The Retail Payments pilot is live at 5 branches (delivered 3 weeks late due to the complexity).
  - Banking transactions - the Ingenico Vocalink ready software release has been provided to Fujitsu (delivered on time).
  - POCA – JPMorgan has completed Vocalink Accreditation (delivered 2 weeks early).
  - Branch communications prepared for PIN pad P2PE anti-tampering / anti-skimming checks that will be needed for the PCI DSS audit (delivered on time).

- Target Operating Model (TOM):
  - Release C: DRSv2 – new reconciliation system is now in use by the Payments Pilot for Global Payments reconciliation and settlement (delivered on time).
  - Release D: Travel Money Card – Development has been contracted with Fujitsu and FRES for implemented (Delivered on time – new plan).
  - Release I: BIN6 workaround to the Ingenico solution - design completed (delivered on time).
  - Release G (delivered on time):
    - ePortal and Ingenico tokenisation being implemented.
    - Financial Crime Team detokenisation application developed.
- Pivot to Cloud. Working closely with the Pivot to Cloud team to manage dependencies due to overlapping timescales.

IT workstream

- The launch of the Payments Pilot in this period is a significant success as it proves the Ingenico integration to Horizon.
- The Fujitsu / Ingenico software development is tracking 3 weeks later than the overall IT workstream plan compared with the last report. This is mostly due to Fujitsu underestimating the complexity of its development and the subsequent additional effort to complete the payments pilot.
- Release 1: Payments Pilot Release:
  - The Fujitsu Retail Payments pilot that was scheduled to commence on 16th November 2020 was implemented on 11 December 2020 at 5 branches.
  - Retail payments are now being successfully made and settled with Global Payments.
- Release 2: Banking Release
  - Ingenico has provided a Vocalink ready release to Fujitsu for integration into Horizon. SV&I testing is targeted to start on 23 December 2020.

Confidential

POL00423694

- POca – JPMorgan has completed the development of its migration to the banking framework.

- Good progress has been made with the Service contract with no major issues outstanding. This activity is now expected to complete governance and sign off in January 2021.
- A standing executive meeting now occurs every 6 weeks with Executives from both POL (Nick Read & Jeff Smyth) and Ingenico (Dan Martensson, VP Global Enterprise Sales & Regional Marketing, and Paula Felstead, Global CTO). Ingenico continues to provide commitment to achieve full accreditation with Vocalink by the end of January 2021.

Target Operating Model (TOM) Workstream Update

The focus of the Target Operating Model workstream is to review the Products and Processes that use Cardholder Data and to remediate and remove them from the scope of the PCI DSS audit where possible. If removal of Cardholder data is not possible then PCI DSS controls will be put in place. A plan has been prepared to remediate the products and processes.

- High Level Solution Design HLD v3.0 has been approved by EAG and it now includes Mimecast / Office 365 Data Loss Prevention (DLP) rules to detect unapproved transmission of cardholder data.
- Release C: A new Data Reconciliation (DRSv2) service has been built and is being used for the Payments pilot with Global Payments.
- Release F (Quatrix / Mimecast / Office365): Mimecast /Office 365: Further work has been ongoing to implement DLP alerting rules and ensure Security Operations are ready for BAU activities. Quatrix – a further scan is planned for January.
- Release G: The Ingenico solution will now include the tokenisation of PANs which is now being implemented. This will enable all enquiries in ePortal to be made using a proxy for the PANs. This tokenisation will also be needed for the TMC solution. A detokenisation service will be needed by the Financial Crime team to access the Full PANs for investigative purposes. Accenture has now built the detokenisation application that will be hosted in AWS.
- Release I: BIN >6 digits workaround. Post Office banking products use BIN ranges greater than the six digits but the Ingenico product does not process more than six digits. The Post Office team has worked with the business to adjust banking products and processes. However, a substantial workaround solution still needs to be put in place. This complex workaround is now being commissioned with Fujitsu, ATOS, Vocalink and Accenture.
- Branch communications have been prepared for January to cover the Anti-tampering and Anti-skimming PIN pad checks that need to be made monthly by the branches. We will also be asking the area managers to support this compliance requirement.

POL00423694

2. What are the key risks & issues on the programme?

The following are identified as key risks:

Risk: There is a high risk and that IRRELEVANT cannot migrate services to route through Vocalink within the timescales and this will significantly affect the programme.
Mitigation: Post Office team is working closely with IRRELEVANT to produce proposals including costs and timescales. IRRELEVANT has allocated resources to scope the work but this is running at a slow pace. The Post Office Director of Banking Services has been made aware of the issue and escalation meetings are taking place. Jan 21 update: IRRELEVANT is indicating that they cannot implement the required change unti IRRELEVANT. A director level meeting is scheduled for the first week of January to see if this delay can be mitigated.

Risk: Due to the complexity of the solution further funds will be needed. Fujitsu is forecasting an overspend; further funds will also be needed to accommodate the change in delivery approach. The contract is T&M and there is a risk of further overspend.
Mitigation: Post Office has challenged the forecast overspend with Fujitsu and will continue to track and manage this issue. Further funding will be needed. Jan 21 update: A change request has been raised to cover the additional funding for the known costs.

Risk: There is a risk that any changes needed to the Fujitsu/Ingenico software will impact the plan. Fujitsu and Ingenico have given a commitment to meeting the current timescales on the basis of no further changes.
Mitigation: Post Office has managed to descope some of the changes identified by working with the business. At steerco it was agreed to implement two of the essential changes – BIN>6 processing workaround and Ingenico tokenisation. TMC could not be accommodated and so this will be delivered as a separate release. The steerco decision aims to keep the implementation of the P2PE solution for banking on track but there will be a delay to the PCI DSS compliance completion.

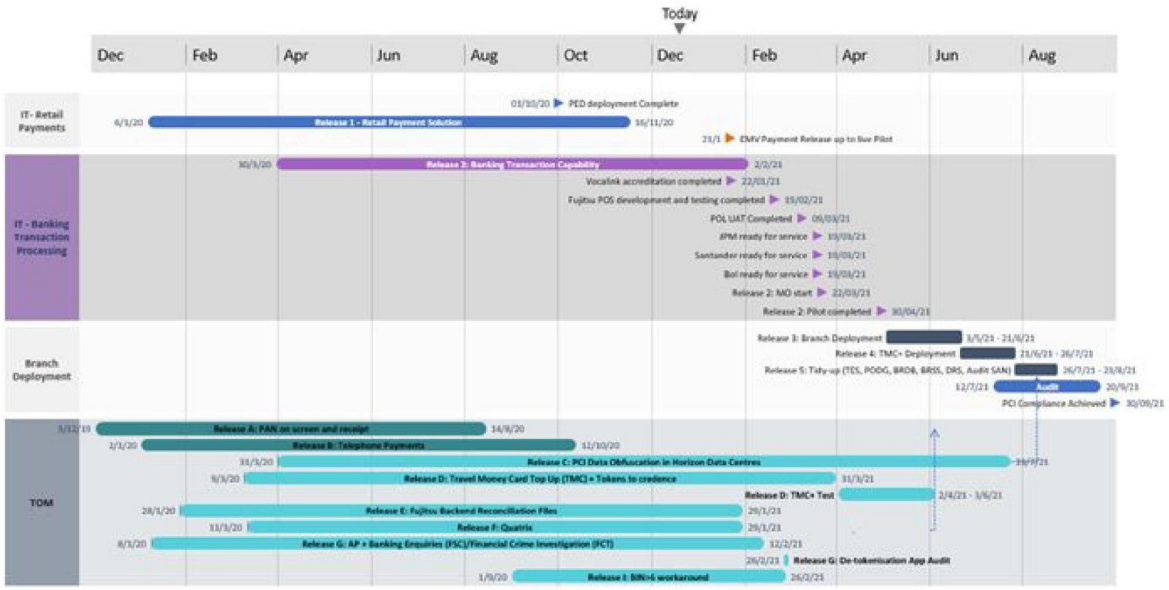
Risk: Bank of Ireland / Instant Saver. Due to the limitation in the Ingenico product to be able to process BIN ranges greater than 6 digits we have had to ask Bank of Ireland to implement a £10k deposit limit in their systems. There is a high risk that they cannot implement this within our timescales which would delay the overall programme.
Mitigation: Post Office is working with BoI/IS to plan the migration. Early information indicates that their development may not be complete until June 2021 at the earliest which would directly impact the plan.

Risk: There is a risk that Coronavirus may impact the delivery timescales for any supplier across the entire PCI programme.
Mitigation: Post Office is working with all engaged suppliers to better understand their contingency plans to ensure that delivery momentum is maintained. This includes the examination of options to minimise delivery impact by understanding key delivery person risks, supply chain risks and other indirect or latent dependency factors.

Confidential

POL00423694

Appendix 1: Programme plan – Current plan including the 3-week Fujitsu Banking Pilot delay.



Confidential

POL00423694

Appendix 2

TOM Workstream Dashboard

	Name	Complexity	Suppliers & Commercials													End-to-End Delivery						
			IUK	FJ	CC	VL	ATOS	Verz	Global	AMEX	FRES	Qtx	M cast	NCC	ACC	Sant.	Discovery	Design	Build	Test	Service Readiness	Deploy	Complete
Release A: Obfuscation of PAN on screen and receipt	PS1: One4All Gift Cards	M		X			X										03/12/2019	23/03/2020	15/05/2020	29/06/2020	01/07/2020	24/07/2020	14/08/2020
	PS1: Travel Money Multi Currency Card	M		X			X										03/12/2019	23/03/2020	15/05/2020	29/06/2020	01/07/2020	24/07/2020	14/08/2020
	PS1: Pre-Paid Debit Cards	M		X			X										03/12/2019	23/03/2020	15/05/2020	29/06/2020	01/07/2020	24/07/2020	14/08/2020
	PS1: Bank of Ireland (cc is decommissioned)	M		X			X										03/12/2019	23/03/2020	15/05/2020	29/06/2020	01/07/2020	24/07/2020	14/08/2020
	PS1: Payment of Santander Credit Card Bill (de-scoped)	M		X			X									X	03/12/2019	N/A	N/A	N/A	N/A	N/A	N/A
	PS1: Budget Card (de-scoped)	M		X			X									X	03/12/2019	N/A	N/A	N/A	N/A	N/A	N/A
Release B: Telephony	PS1: Telephone Payments and Refunds	M						X	X								29/01/2020	19/06/2020	28/08/2020	16/09/2020	21/09/2020	25/09/2020	09/10/2020
	PS2: Storage of Telephone Recordings	H						X									30/01/2020	19/06/2020	N/A	N/A	N/A	N/A	N/A
Release C: Data Obfuscation in Horizon DCs	Audit SAN Legacy Data Obfuscation	M		X													31/03/2020	29/01/2021	26/02/2021	30/04/2021	14/05/2021	09/07/2020	23/07/2020
	BRSS Data Obfuscation	M		X													31/03/2020	15/01/2021	01/06/2021	24/06/2021	24/06/2021	01/07/2021	08/07/2021
	TES Data Obfuscation	M		X													31/03/2020	27/08/2020	26/02/2021	30/04/2021	14/05/2021	09/07/2020	23/07/2020
	PODG Data Scan and PCI Data Obfuscation	M												X			31/03/2020	27/08/2020	17/02/2021	N/A	N/A	N/A	N/A
	PODG Data Scan Mop Up	M												X			31/03/2020	27/08/2020	26/02/2021	30/04/2021	14/05/2021	09/07/2020	23/07/2020
Release D: Travel Money Card	Tactical Money Card Solution	M		X			X				X						31/03/2020	09/07/2020	N/A	N/A	N/A	N/A	N/A
	Strategic Money Card Solution	H	X	X			X		X		X						09/03/2020	29/01/2021	26/02/2021	30/04/2021	14/05/2021	09/07/2020	23/07/2020
Release E: Fujitsu Back End Reconciliation Files	DRS to Accept Obfuscated Rec Files (DRS v.2)	M		X			X										11/03/2020	27/08/2020	18/12/2020	N/A	N/A	N/A	N/A
	Vocalink Rec File Obfuscation	L		X		X	X		X	X							11/03/2020	26/06/2020	N/A	N/A	N/A	N/A	N/A
	Amex and GP Rec File Obfuscation	L		X		X	X		X	X							11/03/2020	26/06/2020	09/07/2021	14/07/2021	N/A	16/07/2021	23/07/2021
Release F: Quatrix, Mimecast, Email	Quatrix storage of PCI data	M										X					11/03/2020	26/06/2020	02/07/2020	09/07/2020	13/07/2020	16/07/2020	23/07/2020
	Transmission of PCI data (Mimecast & O365)	M											X				11/03/2020	18/12/2020	TBC	TBC	TBC	TBC	TBC
Release G: AP Enquiries, Banking Enq + FCT	PS1: ePortal Tokenisation of Full PAN	M	X	X													28/01/2020	20/11/2020	18/12/2020	18/02/2021	04/03/2021	31/03/2021	14/04/2021
	PS2: Ingenico transmission of Full PANs to and from Banks and clients	M															28/01/2020	N/A	N/A	N/A	N/A	N/A	N/A
	Clean Room CDE Environment	M													X		28/01/2020	13/08/2020	04/01/2021	15/02/2021	22/02/2021	25/02/2021	28/01/2021
Release I: >6 Digit BIN Reference Changes	>6 digit BIN Reference Data Changes	M		X			X										27/08/2020	03/12/2020	18/12/2020	18/02/2020	03/03/2020	10/03/2020	17/03/2020
	Building routing table	M					X										27/08/2020	11/12/2020	TBC	TBC	TBC	TBC	TBC
	Vocalink BINn Report	L		X		X	X										27/08/2020	18/12/2020	TBC	TBC	TBC	TBC	TBC
	Vocalink Reapportionment Report Delivery	L		X		X	X										27/08/2020	11/01/2021	TBC	TBC	TBC	TBC	TBC
	Vocalink filtering to maintain routing at BINn Level	M				X											27/08/2020	03/12/2020	TBC	TBC	TBC	TBC	TBC
	Bank of Ireland changes to Instant Saver product	M		X			X										27/08/2020	08/01/2021	TBC	TBC	TBC	TBC	TBC
Other	Prepaid Debit Card Top Ups via banking deposit	M		X		X	X										30/03/2020	25/06/2020	19/03/2021	02/04/2021	09/04/2021	16/04/2021	30/04/2021
	File Data Storage (Data scan)	L		X	X										X		31/03/2020	27/08/2020	29/01/2021	N/A	N/A	N/A	N/A
	Accenture POL SAP Archives	L													X		31/03/2020	N/A	N/A	N/A	N/A	N/A	N/A
	Fujitsu POL SAP Archives	L		X													31/03/2020	N/A	N/A	N/A	N/A	N/A	N/A
	Credence: Fujitsu metadata table BRDB_APS_Prod_SanitSe	L		X													31/03/2020	24/06/2020	17/07/2020	31/07/2020	07/08/2020	21/08/2020	04/09/2020
	Credence: Accenture Varchar obfuscation of PCI data	S													X		31/03/2020	24/06/2020	16/10/2020	23/10/2020	N/A	30/10/2020	06/11/2020
	Credence: Obfuscation of existing PCI data - Tokenisation into Credence	L		X											X		31/03/2020	23/06/2020	26/02/2021	30/04/2021	14/05/2021	09/07/2020	23/07/2020
	POL Forms, documents and branch receipts	M															31/03/2020	27/08/2020	26/10/2020	09/11/2020	23/11/2020	31/01/2021	07/02/2021
	AP-ADC New or Changed Scripts	L		X			X										31/03/2020	17/08/2020	N/A	N/A	N/A	N/A	N/A
	AP-ADC Redundant Scripts	L		X			X										31/03/2020	26/06/2020	02/10/2020	N/A	N/A	18/12/2020	08/01/2021
	Atos Test Environments	L		X			X										31/03/2020	N/A	N/A	N/A	N/A	N/A	N/A
	SPO CEF Recommendations	L															31/03/2020	01/07/2020	31/07/2020	N/A	N/A	31/07/2020	07/08/2020
	Learning & Development Training Materials	L															31/03/2020	19/06/2020	17/07/2020	N/A	N/A	24/07/2020	31/07/2020

End-to-End Delivery Key	
RAG Status	**Delivery Status**
Red	Delivery is outside of tolerance
Amber	Delivery is at risk of moving out of tolerance
Green	Delivery is on track
Blue	Delivery has been completed
Grey	Delivery has not been started

Suppliers & Commercials Key	
RAG Status	**Commercials Status**
Red	Commercials are delayed
Amber	Risk of Delay to Commercials
Green	Commercials are on track
Blue	Commercials have been agreed/signed
Grey	Commercials have not started

Complexity Key		
	# Changes	**# of 3rd Parties**
Low	0-1	0-1
Medium	2-4	2-3
High	>5	>3

Confidential

POL00423694

Appendix 3 Finance Summary

The latest forecast below was presented to the PCI programme steering committee in December 2020.

PCI Programme Capex & Exceptional Spend (2018-2022)	Spend (to end Mar '20)	Actuals (Apr-Nov'20)	F/Cast (Dec'20-Mar'21)	F/Cast 2021/22	LIFE
Internal Labour	£142,589	£423,323	£231,893	£302,781	£1,100,585
External Labour	£1,016,232	£316,429	£150,726	£200,875	£1,684,262
3rd Party Costs	£3,727,554	£5,935,133	£2,779,386	£2,803,026	£15,245,099
Exceptional Costs	£115,000	£0	£0	£0	£115,000
Actual / Forecast	**£5,001,374**	**£6,674,885**	**£3,162,005**	**£3,306,682**	**£18,144,946**
3rd Party Costs Comprise					
Fujitsu	£1,955,216	£4,370,432	£1,688,432	£2,121,286	£10,135,366
Computacenter UK Ltd	£1,342,114	£433,525	£56,660	£103,794	£1,936,093
Atos	£202,011	£554,078	£422,733	£386,000	£1,564,822
Vocalink	£37,437	£203,969	£202,178	£0	£443,584
Other / TBC	£190,775	£373,129	£409,384	£191,945	£1,165,233
Actual / Forecast	**£3,727,554**	**£5,935,133**	**£2,779,387**	**£2,803,025**	**£15,245,099**

The table below shows the breakdown of the IRRELEVANT of cost risk

Workstream	Costs description	Supplier	Nov '20 Forecast (£)	Certainty (%)	Opportunity / Risk (£)	Commentary
IT/TOM	IRRELEVANT					
IT/TOM						
IT/TOM						
IT						
TOM						
Programme						
IT						
TOM						
IT						
TOM						
IT	Fujitsu P2PE - remaining forecast spend	Fujitsu	1,726,803	85	259,020	Fujitsu forecast T&M costs have been increasing. There is a high risk of further increases.
IT	Tokenisation flow through to Horizon / Credence	Fujitsu	70,000	70	21,000	We have a solution identified for the flow of tokens to Horizon, We are awaiting final quotes for the work which should be available by December 2020.
TOM	IRRELEVANT					
IT						

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

4.2

Title:	Cyber Security Update	**Meeting Date:**	12 January 2021
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Group CIO

Input Sought: Noting

The Committee is asked to note the status and plans regarding the reduction of risk associated with Cyber Security including the Crown Jewels analysis for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

Rolling item at each Committee.

Executive Summary

- We continue with our programme of work to develop higher levels of cyber maturity. Progress continues on track in all areas. We include a brief description of our crown jewels analysis for approval.
- We describe the nature of the other Global pandemic – that caused by the Solar Winds attack, the impact on Post Office Limited (POL) and what we are doing next to safeguard against such attacks.
- Our current cyber operations dashboard shows that phishing and data exfiltration from our network continue to be our main issues. More joint and across the board effort is needed to establish a cyber-aware culture.

Questions addressed

1. What is the latest update on the cyber programme?
2. What have we done regarding analysing our crown jewels
    a. What is a crown jewel system and why is it useful to know them?
    b. What are the key roles associated with good IT Controls around crown jewels?
    c. What are our crown jewels?
3. What is the impact of the Solar Winds attack on POL?
4. What are the highlights from the current Cyber Operations dashboard?

Confidential

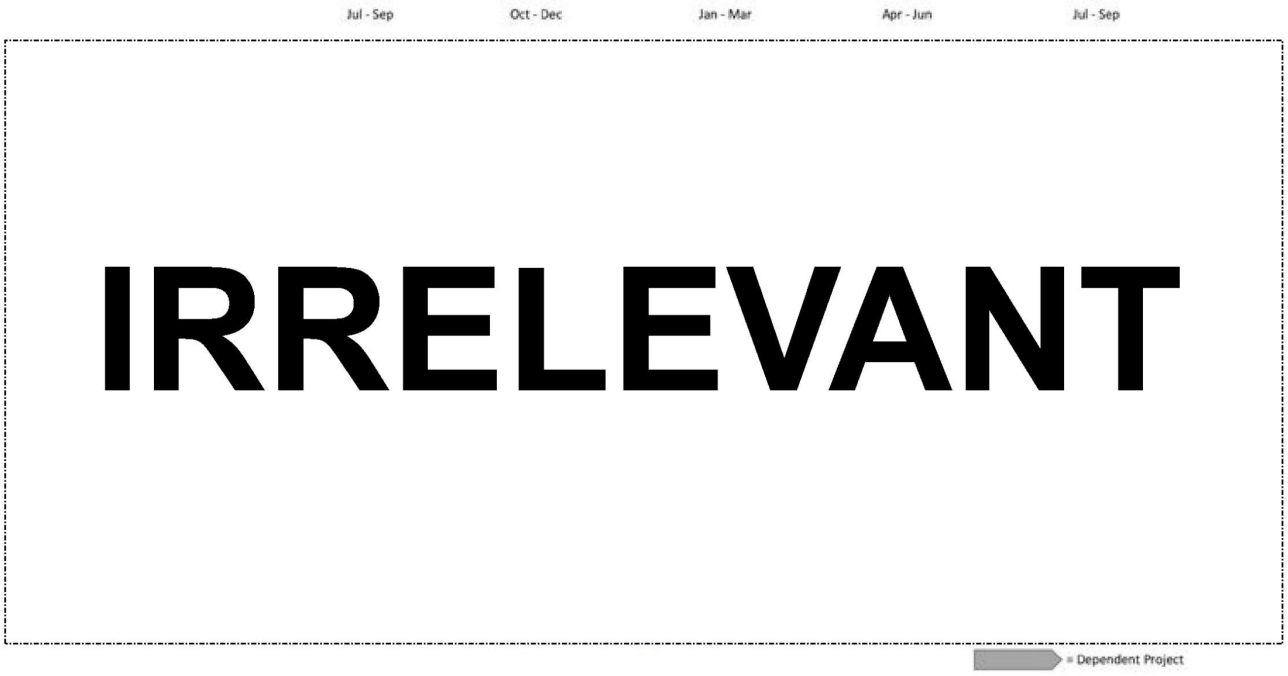
POL00423694

Report: Programme Update

1. The Status of the actions from the recent cyber maturity audit is as per the table below all are complete or on track within target dates

Finding	Status	Target Date
Target maturity levels for cyber security should reflect POL's risk profile	**Completed** – target maturity levels to stay as is unless risk appetite changes significantly	30/9/20
POL's list of crown jewels should be agreed with the business	**For approval**	30/11/20
Security architecture is not fully documented	**In Progress**	28/2/21 revised date
There is no documented long-term cyber strategy	**Completed** – next update Q2 2021	31/12/20
There is no end-to-end programme defined for Cyber	**In Progress** – being developed in line with 21/22 planning cycle	31/3/21
The cyber action tracker requires updating	**Completed**	30/9/20
JML processes are not fully integrated	**Covered under JML paper** – requirement is to introduce automation of workflow where feasible	31/3/21
There is no documented strategy for Cloud security	**In progress**	28/2/21 revised date

2. The roadmap for the cyber programme and dependencies is show below



Confidential

POL00423694

Crown Jewels

3. A crown jewel is a system or system that:
    a. Supports major revenue streams e.g., Horizon.
    b. Supports our ability to function effectively as a business, e.g., Office 365.
    c. Supports our purpose of being there in person.
    d. Any outage or other event would cause adverse media interest.

4. The aim of identifying our crown jewels is to provide a risk-based focus for
    a. Targeting investment for maintenance and development.
    b. Improving cyber defences and monitoring.
    c. IT and management controls improvement.

5. The requirement to identify them and approve them at RCC level was a requirement from the last Deloitte Cyber Maturity Audit.

6. The key roles associated with each crown jewel are:
    a. ***System Platform Owner (SPO)*** – meaning the person that is responsible for maintaining the IT capability of a system. This role is responsible for planning, maintenance, operations, and through-life management of the platform. This is normally a single person.

    b. ***Business Data Owner (BDO)*** – the person or persons responsible for the stewardship of the data on the platform. There can be several people who have this responsibility for a system – especially in cases where multiple tenants use the platform. An example of this is Service NOW which has BDOs across IT, Compliance, Cyber Security and Branch Hub. A key requirement for the BDO is to interpret the data retention requirements for the data they steward using the POL Data Retention Policy as guidance. BDOs are also responsible for data access recertification to ensure that only those who need data have access to it.

7. A list of our crown jewels along with SPO and BDO names is included at Appendix 1.

Report : What is the impact of the Solar Winds Attack on POL?

What has happened ?

8. Solar Winds are a global vendor of IT management software. They are based in the USA with over 3200 employees world-wide serving 320,000 customers in 190+ countries. They are rated number 1 in Network Management by analysts IDC. They are a major player in the technology supply chain.

9. During September 2019 there was a breach of the integrity of the Solar Winds patch process whereby a piece of malware was installed within a software patch for their Orion monitoring product. At this stage the source has yet to be attributed but NCSC state that this is almost certainly a nation state.

POL00423694

10. That patch was then issued to customers starting in March 2020 with 18,000 Orion customers receiving the patch worldwide. There is therefore the potential for widespread infection as the patches are applied to customer networks.

11. On 8 December 2020 FireEye, a US-based Cyber Red Team and Incident Response organisation, publicly announced that they had a major breach associated with the Solar Winds patch where the attacker stole IP including red-team toolkits. Since then FireEye have been working closely with intelligence organisations to assess the extent of the breach. Collectively they have uncovered a widespread campaign that includes victims in USA, Europe, Asia and the Middle East.

12. The attack is currently active in other organisations. NCSC state they have no evidence of impact in the UK but they are working with Government, Critical National Infrastructure and Health sectors where there is known usage of Solar Winds products.

13. FireEye have provided details of technical countermeasures and indicators of compromise for Security Operations Centres (SOCs) to enable them to deal with any infection.

What we have done in response to this attack?

14. We have confirmed with our major third parties that there is no exposure to POL assets as they do not use Solar Winds products on our account. We will continue to work with them to monitor the threat and stay alert to any impact on Post Office.

15. We have confirmed that we do not use Solar Winds products internally and have confirmed this to BEIS.

16. We are providing assurances in turn to our business customers on demand.

17. We have contacted out Cyber Threat Intelligence (CTI) provider who are monitoring the attack for any impact to us.

18. Our SOC has the indicators of compromise that would allow it to spot any infection within the monitored estate and are in contact with our 3rd parties SOCs.

What does this mean for us and what do we need to do now?

19. Whilst there is no known impact to us from this specific attack there may be more like this to come. Sophisticated attackers that are well-resourced will always have the upper hand when it comes to these kinds of attacks - they just have to get it right once whereas we only need to get it right every time.

20. It is also worth noting that this attack may not have been aimed at one organisation specifically – given the attack method involved then it is more likely that an attacker was using it to generate a range of possible openings. For us this means that, as in many scenarios, we may not be the target but we could become a victim inadvertently.

POL00423694

21. Our cyber defences are split across the following categories (an approach known as *defence in depth*)

IRRELEVANT

4.2

22. With such sophisticated attackers out there we are adopting the stance of "it's not if we get attacked but when". With that in mind we are focusing in our 21/22 cyber programme in all defence in depth areas but with more emphasis on c and d above.

23. We will provide details of the measures we are proposing in the next paper but they will include the more widespread use of drills and exercises across ourselves and our third parties and the need for an incident response reserve pool that can be deployed rapidly to get skilled people in place to get back to normal rapidly after any attack.

Report: What are the highlights from the Current cyber dashboard?

24. Appendix 2 shows the current cyber operational metrics dashboard.

25. Key points to note are:

IRRELEVANT

POL00423694

Appendix 1 Crown Jewels Analysis

IRRELEVANT

Confidential

POL00423694

Appendix 2 Cyber Dashboard

Post Office Limited - Document Classification: INTERNAL

Cyber Operations 1

Threat Landscape (Cyber Perspective)

IRRELEVANT

Vulnerabilities (Accenture and CC)

IRRELEVANT



Phishing Protection (AI and

IRRELEVANT

Security Posture

IRRELEVANT

Phishing overview last four campaigns

IRRELEVANT

Phishing campaign Training Compliance

IRRELEVANT

1

Confidential

POL00423694

Post Office Limited - Document Classification: INTERNAL

Cyber Operations 2

IRRELEVANT

- (SOC) Security Email enquiries
- (SOC) PKI Platform (certificates)
- (SOC) Service Now (incidents investigated)
- (SOC) Service Catalogue Enquiries/ Tickets
- (SOC) Phishing Emails Investigated
- (SOC) Escalated from ASOC to POL SOC
- (SOC) Skybox Remediation's
- (ASOC) Processed Incidents Investigated

Cyber Major Incidents of note:

IRRELEVANT

Mail Filtering

IRRELEVANT

- Automated Rejections
- Legit In-bound Email
- Total Outbound Email

Insider Threat

IRRELEVANT

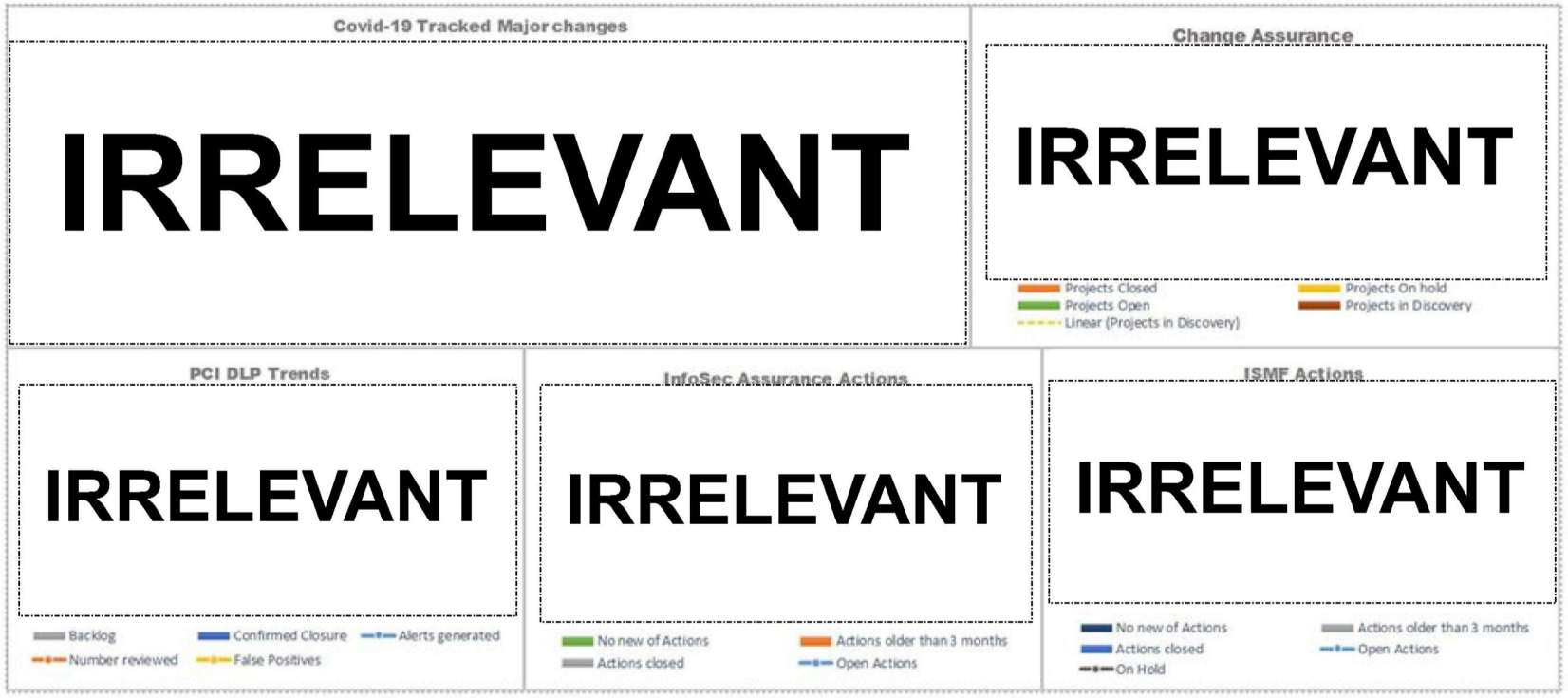
2

Confidential

POL00423694

Post Office Limited - Document Classification: INTERNAL

Cyber Compliance and Assurance



3

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

4.3

Title:	Joiners, Movers, Leavers Update	**Meeting Date:**	12 January 2021
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Group CIO

Input Sought: Noting

The Committee is asked to note the status and plans regarding the reduction of risk associated with Joiners, Movers and Leavers (JML) – in particular those associated with Joiners during the current hybrid operating model, for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

Actions to report on this occurred at the previous Risk and Compliance Committee (RCC) meetings.

Executive Summary

In our continued focus on Joiners, Movers, and Leavers we have performed a deep dive on the Joiners process, following on from the previous report's focus on Movers. Our analysis covers a period for which COVID-19 continues to be actively changing our operating model and introducing new challenges. Short term and longer-term actions are included for joiners and an update is provided on the actions raised in the previous papers.

The GLO IT team have in parallel started their investigation into identity and access management across Horizon – an update on their activity Joiners, Movers and Leavers within Horizon is provided.

We have an increasing number of moving parts around JML which need to be managed. To that end we have employed a contract Head of JML to help us shape what good looks like across Post Office Limited (POL), define key metrics to help target identify issues, develop our target operating model and complete the action from the recent audit to develop a roadmap to get us to the target. A JML steering group has been formed at a working level to ensure coordination and resolution of issues.

Confidential

POL00423694

Questions addressed

1. What are the complexities that we need to address associated with the Joiners process?
2. How well have managed those complexities during the period September-November 2020?
3. What are the GLO IT team doing around JML in Horizon?
4. What steps are we taking to improve JML and produce a cohesive plan and roadmap?

Report

1. In this report we are focusing in on the Joiners process for staff and contractors. This follows on from our work in previous reports covering Movers and Leavers.

What are the complexities that we need to address associated with the Joiners process & how well have we managed them?

2. Effectively joining a role has the following key risks, and issues with associated controls:
    a. **People join without background checks being completed**, which could mean individuals with adverse financial, employment or criminal records join the Post Office. This is mitigated through HR processes – the issuance of a contract is subject to vetting. Therefore, this is unlikely to materialise.
    b. **People join and do not have IT kit or access available on day one**, meaning that they cannot work or seek to work from their own home kit and email addresses introducing data leakage issues.
    c. **The way in which kit is provided seems haphazard,** meaning that on joining people receive upwards of 6 separate couriers delivering components of their IT kit. Our equipment comes from a range of suppliers so whilst this may be inconvenient, we cannot change this in the short term. There is also a concern that personal information is held by more couriers than is ideal although all of our couriers are bound by data protection legislation and our standard contractual terms.
    d. **People join and do not have building access** – this has not been analysed due to the low numbers of people requiring access and the additional special arrangements in place for such people.
    e. **People join and do not get paid** – this is not a cyber-related risk as such. Also, this tends to be resolved quickly by the line manager and new staff member when they realise that they have no pay at the end of the month. This risk has not occurred at POL for a number of years due to effective process.

3. Further analysis has been performed on 2.b above for the 42 joiners during the period September to November 2020. All users had their accounts enabled and used from day one. There were some joiners who were contractors joining as permanent staff who already had an account that was useable.

POL00423694

4. For 2.c above then the provision of the kit was reliant on line management ordering it before the individual arrived. For those whose line managers did not order kit in time then there was a delay but individuals were able to work using web access on a home machine in the interim. Like many of the issues connected with leavers and movers then there is a heavy reliance on line management to perform key tasks.

5. In summary, of the three areas in JML then Joiners appears to be the least risky and the most under control.

What are the additional measures the GLO IT Team have put in place around JML in Horizon?

6. A significant part of the IT estate in POL is run by 3rd parties and this is the case for Horizon. Here, the governance of JML is reliant upon attestation through monthly security management meetings with Fujitsu at which they state they have (or have not) met the required security standards across a range of measures including JML and Privileged Access Management.

7. In the current round of Organisation Development we are proposing to increase the size of the cyber compliance team so that it has the capacity to perform additional and deeper data sampling and audits that will serve to increase the assurance around JML.

8. Horizon requires several internal and external parties to maintain the system which is open to errors and mis-communication. Therefore the GLO IT Team have focused on:
    a. Achieving good process governance.
    b. Understanding and defining expected behaviours of the different team roles associated with the JML process.
    c. Using assurance to confirm that our third parties our following our framework and identify any process shortfalls

9. The proposed GLO IT Action plan is shown in Appendix A.

10. Key focus areas in the plan include:

    a. Introducing a culture of awareness as roles are defined across divisions will essential.
    b. New responsibilities will need to be introduced with the introduction of data and system owners. Ensuring we take a pragmatic approach so that our requirements are met with understanding and not a simple box ticking approach.

11. We will report the progress of this as plans unfold in future papers.

Confidential

POL00423694

What steps are we taking to improve JML and produce a cohesive plan and roadmap?

12. We had an outstanding action for ARC which was to check the leavers and movers as a result of the restructure. We have completed the leavers as a result of the November leavers actions. All GE members now receive a monthly leavers report for their areas as a further check that line management have completed their activities correctly.

13. The People Shared Services Centre (PSSC) have identified the list of movers for the OD period and IT are in the process of checking these for changes to access rights – verbal update at meeting

14. On joiners PSSC are introducing a new onboarding process at the end of January 2021 and part of this, prior to any introduction of HR Service Now integration, will be to send an automated e-mail to IT when a new joiner is added to the system. This will allow IT to be pro-active in contacting appropriate managers – a gap identified in previous papers.

15. We have appointed a contractor Head of JML in IT starting in January 2021 to help us shape what good looks like across POL, define key metrics to help target identify issues, develop our target operating model and complete the action from the recent audit to develop a roadmap to get us to the target.

16. A JML steering group has been formed at a working level to ensure coordination and resolution of issues across POL.

POL00423694

Appendix A GLO IT Action Plan

Finding	Category	Deliverables/Scope	Target Date
Scope Area: Process Governance			
No overall IAM governance (e.g. no ownership of the end to end process, no process diagram) IAM–JML access management responsibilities (RACI) and controls are not clearly and transparently defined Line managers not well informed about their responsibilities regarding IAM-JML process Data and system owners have not been identified (responsibilities assigned) Non-compliance with the access control standard/policy	Owners	Identify Business owners Formalise Roles and Responsibilities Build training materials and plan	Q4/Q1 Q1 Q2/Q3
	Process	Document Horizon JML processes Document 3rd Party JML Processes End to end process assessment and redesign	Q4/Q1 Q1 Q2
	Governance	3rd Party Assurance Process (Check contract review, JML key control sample etc) Document governance framework and formalise policy requirements Risk Committee review Assurance process for key controls (internal/3rd party)	Q2 Q1/Q2 Q3 Q2
Scope Area: Joiners' process			
No assurance that access rights are limited to a need to know basis	Review	Map current role based access rights (high level) Gap analysis against requirements (Least access)	Q4/Q1 Q1
	Build	Access rights changes (as required)	Q1/Q2
	Process	Document new access process (prevent cloning of IDs)	Q2
HR does not have a full overview of all parties working for PO (employees, contractors)	Process	Work with HR to enhance their processes	Q2
Scope Area: Movers' process			
No assurance that access rights are reviewed when someone moves role/function Periodical access reviews not in place (for LAN, share drives and all applications)	Process	Document new movers process to provide Check/Challenge	Q2/Q3
Scope area: Leavers' process			
No assurance that leavers' access rights are removed (timely)	Process	Document new Leavers process to provide Check/Challenge	Q2/Q3

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	IT Controls Update	**Meeting Date:**	12 January 2021
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Group CIO

5

Input Sought: Noting

The Committee is asked to note the status and plans regarding the reduction of risk associated with IT Controls for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

Request from Chair of ARC for update at previous ARC meeting.

Executive Summary

We have run formal IT Controls since 2017 using the COBIT5 framework. Every quarter we assess ourselves on those controls and where necessary perform targeted remediation activities, reporting through the IT Leadership Board.

A series of audits have been conducted by Internal Audit with the latest rated as "Needs Improvement". This, combined with our own analysis of areas to focus on and the changes made by recent organisation development activities, will form the action plan for improvements during 2021.

Questions addressed

1. What have we done to date on IT Controls?
2. What is our current status and what are our improvement activities?

Report: What have we done to date on IT Controls?

1. A previous paper in March 2020 provides a detailed view of our controls framework – the highlights are summarised below.

2. The Post Office Limited (POL) IT Controls Framework (ITCF) is based on the internationally recognised COBIT5 framework. The ITCF was put in place during 2017 following a detailed review and recommendations from KPMG.

3. The ITCF has 268 controls across 17 COBIT5 processes that were selected as being the most relevant to POL and the risks being faced at the time of inception.

4. The ITCF provides an ongoing assessment of the operation of controls and any outstanding remediations for control deficiencies, based on quarterly control self-assessments (CSA).

Confidential

POL00423694

5. CSA activity and remediations are tracked using PWC's Traction toolkit. Each CSA is triggered and managed by Cyber Security. The results, escalations and remediation activity raised by the CSA process are reported to the IT Leadership Board (ITLB) for further action.

6. The results from the most recent CSA are included at Appendix 1. These show that 83% of controls are operating effectively. Of the remainder, 10% are not operating effectively and 7% are not being operated due reliance on key people who are absent or have left. For the non-effective and not operated controls there are remediation plans in place with progress being monitored monthly at ITLB.

7. Other control frameworks in use include those for specialist areas such as Cyber Security and Service Management – the assessments from these are fed into the ITCF which sits above all of these.

8. On wider engagement initial meetings have been held with the POL-wide project team on controls to ensure that there is alignment between it and the ITCF.

Report : What is our current status and what are our improvement activities?

9. To understand whether we are doing the right things in the right way Internal Audit have reviewed the ITCF:
    a. During May 2019.
    b. As part of the maintaining minimum control standards review in August 2020.
    c. In December 2020 – the report for this is included by IA at this committee.

10. Internal Audit have concluded the following:
    a. "Significant progress has been made following the implementation of the ITCF in 2018 and the Internal Audit review in 2019, with greater clarity around control operation, increased senior management and control owner engagement, improvements to the TrAction tool that supports the framework, generally increased self-assessment completion rates and enhanced tracking of remediations.

       However, operation of the ITCF has been impacted by key staff absence and support should be provided to minimise this risk in future. Management should continue to refine the design and operation of the ITCF to ensure that control weaknesses are quickly identified and addressed, supported by migration to ServiceNow and robust assurance of control design and operation.

       The ITCF continues to mature but is not yet fully embedded within the business and, therefore, we have rated this report as 'Needs Improvement'."

POL00423694

11. The findings of the latest audit are shown below:

Finding		Rating*	Action Owner	Date
Scope Area: ITCF Design				
1	Not all control activities are aligned with CobiT5	P2	Aatish Shah, IT Governance and Reporting Manager	30 Sep 2021
2	Test scripts are not supported within the ITCF	P2	Aatish Shah, IT Governance and Reporting Manager	30 Sep 2021
Scope Area: ITCF Operation				
3	There is reliance on key staff for maintaining the smooth operation of the ITCF	P2	Aatish Shah, IT Governance and Reporting Manager	28 Feb 2021
4	The current tool does not fully support ITCF operation	P2	Aatish Shah, IT Governance and Reporting Manager	30 Sep 2021
5	There is inconsistent use of the Automated/Manual control field in TrAction	P3	Aatish Shah, IT Governance and Reporting Manager	28 Feb 2021
Scope Area: Control Effectiveness and Ongoing Management				
6	No robust process for is in place to provide second line oversight of the ITCF	P2	Tony Jowett, CISO	30 Jun 2021
7	Controls assessed as 'not operated' may be effective/not effective	P3	Aatish Shah, IT Governance and Reporting Manager	28 Feb 2021

12. In addition to the audit IT have conducted their own assessment of control areas that need further investigation as to their fitness to the current environment based on the risk to our crown jewel assets.

13. Firstly, in response to the work conducted under OD we need to review that we have the correct control ownership across all COBIT 5 processes.

14. IT Controls exist to manage risk. Therefore we are focusing our improvement effort on COBIT 5 controls of greatest risk, namely those areas connected with the management of our 3rd party estate through the lens of our crown jewel systems.

15. We will assess whether the controls are appropriate, at the requisite maturity level and have the right coverage. The COBIT5 processes to be focused on are:

    a. **Manage Suppliers –** starting with coverage of our suppliers running crown jewel systems.
    b. **Manage Service Agreements** – specifically obligation/SLA checking/ making sure we meet business need and define future business needs for inclusion into contracts from a controls perspective.
    c. **Manage Continuity** – as an area that has changed under OD and also has had key-person risk.
    d. **Manage Portfolio** – ensuring that we understand the resource constraints on some of our 3rd parties and manage the risks accordingly with major projects and programmes in those areas.
    e. **Manage Enterprise Architecture** – ensure we have coherence across the estate whilst we go through the necessary changes from major programmes such as Belfast Exit, PCIDSS, EUC and SPM.

16. The above areas will be reviewed internally by the POL controls team using guidance available within the COBIT5 documentation set.

Confidential

POL00423694

17. During Q2 '21 we will perform a second line review for controls appropriateness and maturity (as per the audit action against the same point).

18. In parallel with these efforts the GLO IT team have assessed the controls around Horizon. The findings from this review will be added to the overall controls planning.

19. As part of the OD efforts we are bolstering our capability in controls management to ensure we can sustain the necessary focus in this area.

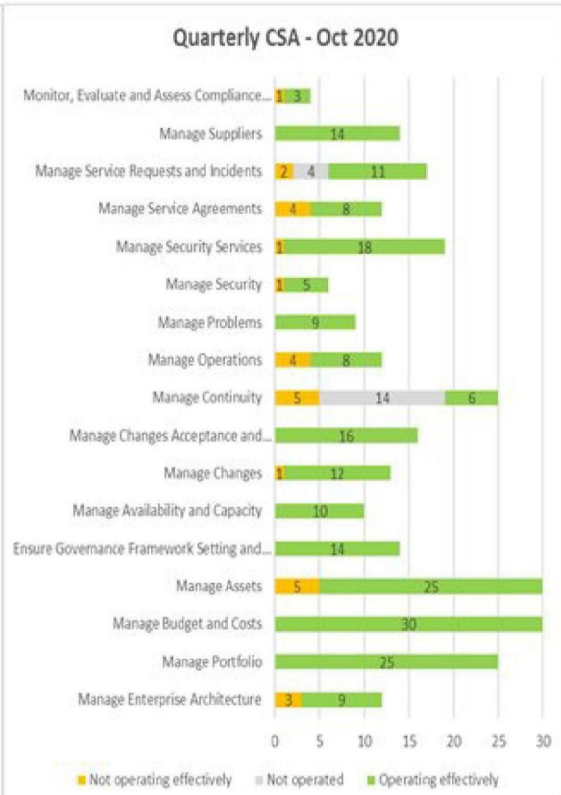
Confidential

POL00423694

Appendix 1 IT Controls Status from October 2020 Self Assessment

IT Controls





Key Update

Control Remediations

- There are in total 44 in-progress remediations due between Dec 2020 to Dec 2021, details included in further slides

Quarterly Control Self Assessment (CSA)

CSA takes place after end of ever quarter. CSA conducted in Oct 2020 for the quarter July – Sep. Of a total of 268 controls issued for review: **All 268 (100%) controls have been assessed.** Out of 268 controls assessed:

- 223 (83.2%) were operating effectively
- 27 (10.1%) were not operating effectively
- 18 (6.7%) were not operated - 14 are linked to "Manage Continuity" (lack of ITSCM Manager)

Other News

- *Annual Internal Audit on ITCF in progress, Report expected in Nov 2020.*
- *Recruitment activity in progress for an IT Governance Analyst to supplement the efforts of our existing IT Governance & Reporting Manager*
- *IT provided their tooling requirements and inputs for the overall business case being facilitated by Risk.*
- *TrAction contract in place till 31st March 2021. SNOW evaluation /commercials being progressed.*
- *Migration data requirements have been agreed with current partner PwC and being discussed with SNOW.*
- *Controls reviews completed with all control owners in September to ensure the controls are up to date. Reduced from 310 to 274 unique IT Controls.*

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Supply Chain Bolton IT Risk Update	**Meeting Date:**	12 January 2021
Author:	Russell Hancock, Supply Chain Director	**Sponsor:**	Al Cameron, Group Chief Finance Officer

Input Sought: Noting

The Committee asked to note the issues highlighted, the steps being taken to identify and reduce any potential risks and to agree on next steps and further updates.

Background

6

As part of the preparation of moving off of the Bark Street Bolton site the IT team were asked to assist the Supply Chain National Cash Account Reconciliation Team (NCCART) on moving some bespoke hardware to the new Bolton site.

The original system was installed as a key part of the closure of Manchester Cash Centre in 2010 with the NCCART team being relocated into Bark Street. The entire relocation appears to have been managed centrally as a property team project with the CCTV relocation subcontracted the Kings Security. It would appear that at no point was the central Post Office IT consulted or advised as part of this project.

IT colleagues discovered that the NCCART team were using a PC in order to access the CCTV systems across the SC cash centre estate, primarily for the purpose of viewing camera footage in relation to disputed branch discrepancy claims. The system gave the user open access to download or view in real time the live CCTV feeds both internally and around building perimeters. This open access link had the potential to make all cash centre locations vulnerable to a planned robbery through being able to identify weak spots in building perimeters, ascertain when maximum cash is exposed and potentially identify colleagues in order to coerce through Tiger Kidnap activity.

The PC concerned also had the following issues when IT team investigated further: -

- No anti-virus running leaving the machine vulnerable to viruses
- No internet security so nothing stopping unauthorised connections or spyware getting access
- No data encryption on hard drive
- Running a non-enterprise operating system meaning the system is never patched or fixed
- No domain so no central management of the PC
- Memory sticks being used to transfer data with no encryption as no Bitlocker on PC.
- Open access to the internet.

Once these issues were identified all of the PCs were removed from site including the memory sticks and CD's and transferred to secure storage at Manchester CVIT depot.

Strictly Confidential

POL00423694

The machines have now been transferred into the custody of KPMG who are currently undertaking a technical forensic examination in order to determine if the machines have been compromised in any way. As of Monday 4th January 2021, their findings to date match the business purpose of the PCs and portable media and there is no evidence to suggest that the PCs and media have been used in any other way or in a way that exposes POL to undue risk. The full examination and report will be published w/c 12th January 2021.

In order to give wider reassurance the IT team were then asked to undertake an audit of all SC sites to ensure that all IT equipment contained within was compliant and posing no risk to PO IT infrastructure, identifiable to IT team and logged on their inventory of equipment and up to date with latest protocols. At present this audit is hallway through completion but the team have identified the following points to be noted: -

Digital CCTV Systems – IRRELEVANT

IRRELEVANT

6

Bodycams & BT Routers – IRRELEVANT

IRRELEVANT

Personal Transfer Unit PC – PTU is a secure method of allowing access into our cash and CVIT units. IRRELEVANT

IRRELEVANT

With over half of all SC sites having now been taken through a thorough on site audit, apart from the unique Bolton risk and the CCTV risk identified above, no other threats or issues have become apparent and I have been assured that Supply Systems are fully compliant.

How did we get to this position?

All of the at risks systems were updated some time ago with the most recent change being the NCCART migration into Bark Street, Bolton and the provision of body worn cameras by CVIT crews.

Without exception all of the at risk equipment identified by IT colleagues had been installed as part of one off bespoke project, managed by either property or security on behalf of the wider business. These projects were completed at a time when Post Office didn't have the level of

POL00423694

change governance that exists today, the activity at the time being managed as a single enclosed project.

As part of our ongoing deep dive we've not be able to find any handover into BAU IT ownership, so this has meant that this particular infrastructure has been sitting outside of IT governance and ownership. We have also struggled to find background data and decision paperwork to identify the methodology used to sign off, fund and implement the programmes that delivered these projects.

As a result of the above, the equipment was installed, tested and once complete, the project team disbanded handing over to BAU teams. Those teams have then just carried on using the systems and tools given to them, assuming that all was correct and configured appropriately as it had been installed by business contractors.

When subsequent IT equipment upgrades have taken place, these machines have been bypassed as they are not included on the fixed asset register of IT equipment. Regrettably none of the operational teams ever challenged that these machines never seemed to have oversight or checking over the course of time.

Next Steps

- Continue the audit of Supply Chain sites concluding in Jan 2021
- Expand the scope of internal Audit to include areas of Supply Chain that have not been traditionally covered (such as cash management team)
- Ensure that audit process is sufficiently varied throughout the year to enable a wider inspection of all aspects of Supply Chain operations and support.
- Creation of an annual Supply Chain online support course that highlights awareness of ensuring process and operating practices are fit for purpose, how to call out when they're not, building upon lessons learnt from audit programme.
- Report back to RCC in March with a further, final update.

Strictly Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Money Laundering Reporting Officer Annual Report	**Meeting Date:**	12 January 2021
Author:	Sally Smith, Money Laundering Reporting Officer & Head of Financial Crime	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Discussion & Approval

The Committee is asked to:

- review and discuss the annual report and its conclusions as part of its role in monitoring the adequacy and effectiveness of the Group's anti-money-laundering systems and controls which ensures Post Office's meets its regulatory obligations under the Money Laundering Regulations; and
- approve the recommendations within paragraphs 9 – 25 of this report and paragraph F of the Annual Report of the Money Laundering Reporting Officer, prior to the Annual Report being issued to our regulator, HMRC;

for onward submission to the Audit, Risk & Compliance Committee (ARC).

7

Previous Governance Oversight

January 2020 Annual MLRO Report and updates via the Risk & Compliance Report at the Risk & Compliance Committee (RCC) and ARC.

Executive Summary

The Money Laundering Regulations (MLRs) require that the Money Laundering Reporting Officer (MLRO) produces an annual report to appraise senior management on the effectiveness of key Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) controls, and make appropriate recommendations for improving the management of risks, priorities and resources, if appropriate.

Questions addressed

1. Is Post Office complying with the requirements of the regulation?
2. What are the key AML and CTF risks within Post Office Ltd and are there any significant gaps or weaknesses in the Post Office's compliance with its regulatory obligations under the Money Laundering Regulations (MLRs)?
3. What are the key activities that need to be undertaken to address these gaps?

Report

4. The full annual report is attached and covers the key reportable regulatory responsibilities under the MLRs. Appendices referred to in the report are in the reading room.

CONFIDENTIAL

POL00423694

Financial Impact

5. Post Office have not received any regulatory penalties since 2017/2018 when HMRC fined us c.£1.1m for regulatory breaches in relation to Travel Money. During 2020, Post Office self-reported a regulatory breach to HMRC in respect of 6 branches that had traded Bureau de Change despite not being registered. HMRC advised they would take no action or sanction against Post Office, but confirmed that they will judge all matters on their individual circumstances and therefore any repeated breaches may result in sanctions.

6. We continue to see increasing scrutiny by regulators in the UK, reflecting the guidance in the last Financial Action Taskforce Mutual Evaluation Review. This year fines of c.£84m have been levied by UK AML regulators, including c.£307k by HMRC.

7. HMRC annual registration fees were c.£1.7m in 2020 and additional costs are associated with Fit & Proper requirements and transaction monitoring and assurance.

Risk Assessment, Mitigations & Legal Implications

8. Products and services provided by Post Office are broadly in line with the risk appetites set by the Board although there continues to be a significant increase in potential money laundering via Banking Framework cash deposit services. There has been an improvement in residual risk over the last 12 months across most products and services.

Conclusions and Recommendations

9. The regulatory environment continues to pose a challenge, with increased regulatory and legislative focus on money laundering and terrorist financing. The 2020 National Risk Assessment (NRA) published in December 2020 demonstrates risks remain high, particularly in relation to cash based services, and calls out in the executive summary the risks associated with banking cash deposits over Post Office counters. We expect HMT to introduce an Economic Crime Levy in 2021, which will increase the regulatory fee burden for Post Office and increase scrutiny from law enforcement and supervisors as funding from the levy is applied to target money laundering risks. **Risks will continue to be monitored by the MLRO, providing regular updates and reporting to the RCC and ARC, and sponsorship of required actions will be required by GE.**

10. Covid-19 has had a significant impact on the Financial Crime landscape, and there has been a general increase in frauds, scams and changes in Organised Criminal Gang's (OCGs) activities. There has been an increase in scams relating to vulnerable customers and we have seen examples of suspicious activity in the Post Office related to Bounce Back Loan (BBL) fraud. The volume of SARs has doubled and investigations have risen by a third in the last 12 months, with no indication that volumes are reducing. **The additional PO grade recruited into the Financial Crime Compliance team in October and funded until the end of 2020/21 will need to be fully funded for 2021/22**.

11. During the year Amazon vouchers were increasingly targeted by fraudsters scamming vulnerable customers. Work has been undertaken to identify tighter controls to mitigate the risks around this Post Office product, however, the Product Manager is a Payzone Bill Payments employee and does not have access to Post Office tools and change procedures, which has meant some delays to required changes. **The Bill Payments/Payzone teams need to identify and implement a solution to this issue, to ensure that the product managers have access to the tools and systems to manage Post Office products.**

12. There has been significant focus over the last 12 months by the National Economic Crime Centre (NECC) and Post Office in addressing the risks relating to cash deposit services, and Post Office needs to be able to demonstrate that it is both aware of the risks and has

POL00423694

controls in place to manage them. In 2020 up to P8 there have been investigations into c. £198m suspicious cash deposits – more than double that for the whole of 2019. We have continued to support the NECC Project Admiralty established to tackle the cash deposit threat over Post Office counters and established a Banking Framework Services AML Sub Group to highlight and discuss the issues with the banks.

13. Cash deposits completed in 2020 relating to Money Transmission Businesses have highlighted an unforeseen issue with businesses that deposit excessive volumes of cash through a single location. Whilst actions have been taken to address the physical security risks associated with these, further consideration is needed to tackle the money laundering placement risks associated with accepting high value cash deposits from high risk businesses. **Robust solutions need to be identified and put in place by the Product Team, with the support of Compliance to ensure that Post Office can demonstrate to regulators, if called upon to do so, that sufficient controls are in place.**

14. The HMRC supervisor who had overseen Post Office regulated activity since 2015 retired in May 2020 following handover to a new supervisor. The new supervisor secured a new role in the summer and a further supervisor was appointed in August. Due to Covid, HMRC are not undertaking any supervisory visits or meetings, and it is unclear what level of scrutiny we may see in 2021. We are also expecting a further consultation on HMRC's fee structure in 2021.

15. Training is a key AML control for Post Office and there have been some instances of poor/late completion of mandatory training by employees and contractors and we still see instances where SARs should have been raised by branches. The resource responsible for training, awareness and communications was transferred to the Communications Team in March 2020, but continued to deliver all aspects of the role. However, the role was removed in November 2020 as a result of OE, and whilst the Communications Team will still support communication activity, the work to support training content will have to be undertaken primarily by Financial Crime Compliance moving forward, and this may impact the ability to further enhance training. **Compliance will monitor training completion more closely in 2021 and further awareness raising via Area Managers will be undertaken.**

16. Both first and second line management have responsibility to ensure that the controls in place work as intended. Quarterly assurance checks against the policy minimum control standards by Financial Crime Compliance evidence that a number of first line controls are only partially effective. **The planned activity in 2021 by Compliance on the Controls Framework should help improve first line understanding and application of their responsibilities.**

17. Products and services provided by Post Office are broadly in line with the risk appetites set by the Board and there has been a general improvement in residual risk over the last 12 months. There have been delays starting the Payzone financial crime risk assessment due to resourcing and funding challenges, but these were resolved in Q3, and recruitment of a fixed term contract Financial Crime Manager to complete the work is progressing. **The Payzone assessment is scheduled to be delivered at the end of the financial year.**

18. A SAR received from one branch identified a complex trading structure with links to overseas money transmission companies via the Bill Payment Services, exposing an issue relating to product understanding of exactly what types of businesses are serviced under re-seller contracts. **The controls relating to Re-seller contracts will be reviewed as part of the Payzone and Bill Payments reviews in 2021.**

CONFIDENTIAL

POL00423694

19. The accredited FIO within Security Operations who assisted with the review of SAR disclosures relating to possible Post Office employees and postmasters has left the business and the replacement resource will not have FIO accreditation. **Financial Crime Compliance will monitor the impact of this additional workload moving forward.**

20. The Post Office PCI DSS Compliance project will impact Financial Crime Compliance adding additional time to some activity, as card data will need to be accessed, processed and stored in a 'clean room' environment. Additionally, during the rollout period, both the existing and new systems will need to be accessed when undertaking investigation work. **Financial Crime Compliance continue to work closely with the project team, and have called out that additional PO resource may need to be funded by the project to support the transition period.**

21. As in 2019, significant challenges with the Fit & Proper project have continued with considerable oversight and support required. The new system for generating annual declarations, capturing data and generating the required reporting for Post Office internal governance and HMRC agent data provision was delivered in July 2020, but there are on-going data integrity issues (resulting on one occasion in requesting from HMRC approval of a late submission of monthly data).The F&P team has moved under a new team leader as a result of OE, therefore the knowledge and expertise built up by the original team leader during the last 6 months will be lost. **Further oversight and work will be required to ensure compliance in 2021, and Internal Audit have been asked to schedule a review of regulatory data requirements for both Fit & Proper and Premises Registration.**

22. Despite improvements relating to direct employee F&P processes implemented in the first half of 2020, the most recent OE changes have made it difficult to keep this up to date as individuals leave the business and role titles/responsibilities and line management changes have occurred. **Financial Crime Compliance will continue to work closely with HR to resolve current discrepancies and implement more robust controls.**

23. Further work has been undertaken to improve and implement Bureau de Change monitoring reports which has led to an increase in cases, despite the reduction in overall transaction volumes caused by Covid. The new reports have enabled the identification of potential vulnerable customers and highlighted customers travelling to multiple branches to purchase currency, further evidencing the improvements in monitoring controls since the HMRC audit in 2016. There continue to be issues with data and reporting around potential Sanctions matches, and whilst there are manual workarounds, Accenture have not yet fixed the underlying issue. Monthly meetings now held with the Travel Money team ensuring they have direct oversight of the activities to support their product, and also ensuring Financial Crime Compliance are kept up to date with any product changes or developments. **Accenture and the Data Centre of Excellence need to identify and implement a fix to the Sanctions data issue. The effectiveness of Bureau de Change monitoring reports will continue to be reviewed by Financial Crime Compliance.**

24. In summary, the framework of AML/CTF controls is generally effective and Post Office is meeting its regulatory requirements under the MLRs. However, there are key areas where focus needs to be maintained to ensure this continues, particularly in relation to:

    i. The general increase in frauds, scams and changes in Organised Criminal Gangs (OCG) activities across industry caused by Covid and the ongoing economic outfall

POL00423694

ii. The maintenance of, and timely and accurate provision to HMRC of agent Fit & Proper data and Premises Registration data, and ensuring that HMRC direct employee checks are kept up to date

iii. The continuing increase in suspicious activity relating to Banking Framework cash deposits, and the increase in the size of some business cash deposits

iv. Ensuring there is sufficient resource within Financial Crime Compliance to manage the increasing Bureau de Change, SAR, investigation and product and service risk assessment workloads

25. Additionally, attention needs to be focused to ensure that:

i. Key training messages can still be delivered and have been understood

ii. First line are aware of their responsibilities to operate their functions and activities in line with policy minimum control standards

CONFIDENTIAL

POL00423694

The Annual Report of the Money Laundering Reporting Officer for the Post Office Limited for the period 1st January 2020 – 31st December 2020

Table of Contents

A. Purpose and Scope of Report
B. Governance Framework
C. Operation and Effectiveness of the Control Framework
  i. Senior management oversight
  ii. Staff awareness and training
  iii. Risk assessment, policies, controls and procedures
  iv. New products and services
  v. High risk products and services
  vi. Customer due diligence requirements
  vii. Reporting suspicious activity
  viii. Record keeping
  ix. Premises Registration
  x. Fit & Proper tests
D. Incidents and Investigations
E. External Threats/Landscape
  i. Business areas
  ii. The 4th Money Laundering Directive
  iii. The 5th Money Laundering Directive
  iv. The Criminal Finances Act 2017
  v. The Policing and Crime Act 2017
  vi. Joint Money Laundering Intelligence Taskforce
F. Conclusions and Recommendations
Appendix A: Post Office Insurance annual MLRO report
Appendix B: Product and Service Risk Assessment Summary
Appendix C: Summary of UK Enforcement Action
Appendix D: Product and Service Risk Exceptions
Appendix E: Report on duties of Nominated Officer – Suspicious Activity Report Summary

7

A. Purpose and Scope of Report

1. As required by the Money Laundering Regulations (MLRs) this report appraises senior management on the effectiveness of key Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) controls and their application, and makes recommendations for improving the management of risks, priorities and resources.

2. HMRC is the regulator responsible for supervising Post Office Limited (POL) compliance with MLR requirements. Their oversight relates to POL Money Service Business (MSB) activity, specifically, the provision of Bureau de Change.

3. Organisations are required to adopt a risk-based approach to prevent money laundering and terrorist financing. Risk assessment must be documented and evidence the decisions that senior management have made in the context of the particular risks facing the business.

4. POL is required, both contractually and under the MLRs, to have in place and comply with policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing for all the products and services it offers through third party or white label solutions and joint venture arrangements (e.g. MoneyGram, Banking Framework Services, financial services products, Gift Cards, etc.).

POL00423694

5. The most significant impact of financial crime for Post Office continues to be reputational damage. Negative media attention following an incident has potential for loss of consumer and client confidence in the product/service, consequential devaluation of brand values and possible impact on Government commitment which is vital to support Post Office.
6. The MLRO and the Financial Crime Compliance team are responsible for financial crime policies, assurance and AML/CTF risk assessment of products and services *(see Section C and Appendix B).*
7. Post Office have not received any regulatory penalties since 2017/2018 when HMRC fined us £796,500 in respect of premises registration errors, and £344,766 for regulatory breaches in relation to oversight and risk assessment of Travel Money, but we continue to see increasing scrutiny by regulators in the UK, and c.£84m of fines have been levied on firms by UK regulators in 2020, including c.£307k by HMRC *(see Appendix C for summary of UK enforcement action)*
8. Post Office Insurance is subject to a separate MLRO annual report each year, which can be found in Appendix A.

B. Governance - those responsible for anti-money laundering systems and controls, and the structure within which they operate

9. Ben Foat is the GE member and officer appointed to be responsible for overseeing compliance with the MLRs.
10. Sally Smith is the MLRO and a member of the Post Office Compliance team and is ordinarily located in Finsbury Dials, Moorgate, London, where Post Office Group is situated. The MLRO takes ultimate responsibility for compliance with the MLRs, the provision of training and awareness within Post Office, the design and implementation of internal anti-money laundering policy, systems and procedures, and advising on how to proceed once an internal report and/or Suspicious Activity Report (SAR) has been made.
11. Under the direction of the MLRO, POL's exposure to financial crime is assessed and assured. This includes
    - setting policies and standards relating to financial crime, assessing and assuring AML/CTF risks across Post Office;
    - ensuring that risks are properly reflected in Risk & Controls Matrices (RACMs);
    - ensuring appropriate disclosure of SARs to the National Crime Agency (NCA);
    - liaising with third parties regarding investigations; and
    - ensuring information is appropriately disclosed to clients or third parties.
12. Through the Financial Crime Compliance team, the MLRO has oversight of AML/CTF investigations, non-conformance by branches or individuals and risk assessment of products and services.
13. During 2020 regular reports have been provided to the Risk & Compliance Committee (RCC) and the Audit, Risk & Compliance Committee (ARC) covering AML/CTF controls, the outcomes of risk assessment work, HMRC supervisory activity, changes to legislation and industry issues.
14. Changes in economic crime activity driven by Covid and increased banking cash deposits have increased workloads significantly, and an additional PO grade was recruited in October on a fixed term contract to the end of the 2020/21 financial year. This resource

POL00423694

will be required on a permanent basis from 2021/22 as SAR and investigation volumes have continued to be much higher than in previous years. *(see paras 46-47 and Section D)*

15. Other than for Bureau de Change, financial crime MI reporting within Post Office is still not sufficiently granular at product level to aid transparency and decision making, although there have been some improvements with Banking MI and more are being investigated. Product specific monthly MI on the work undertaken by Financial Crime Compliance is shared with the Travel Money Product Director. Consistency of information and analysis capability for other products and services makes it harder to appropriately balance commercial considerations against regulatory risks, although these are lower risk products, and Post Office is not directly regulated for them.

C. Operation and Effectiveness of Control Framework

i. Senior management oversight

16. See Section B above for summary of governance and oversight.

17. HMRC Fit and Proper tests must be performed on all external Board Directors, GE, the MLRO and impacted employee roles as per HMRC requirements and Post Office policy, although there have been challenges during the recent restructure *(see para 69).*

ii. Staff awareness and training

18. Awareness and training is a key control for Post Office, and annual training was updated to cover issues and incidents that had arisen in the previous 12 months. All staff are required to complete AML/CTF training:
    - Back office employees must complete within 30 days of joining and annually
    - Customer facing employees and agent assistants must complete before they have access to Horizon and annually

19. Monitoring of training completion levels for back office staff is undertaken by HR Directors, and those staff who do not complete mandatory compliance training are dealt with via conduct with potential removal of annual bonus payment. Training completion is subject to quarterly assurance checks by Compliance. During 2020, there have been a number of occasions when completion rates have been below 95%, primarily due to non-completion by contractors, although there have been a couple of individuals who have failed to complete compliance training. These individuals have been chased by Learning & Development and new controls are being identified for contractors to ensure timely completion.

20. Annual training was completed between 1st and 26th May 2020, although due to Covid, branches were given an extension until 14th July 2020 to complete the training.

21. We have been working closely with Area Managers to raise awareness of emerging trends and issues, and the higher volume of SARs received from the network and CViT in 2020, seems to indicate that key areas of training are being understood and acted upon, although there are still occasions where SARs are not being raised.

22. 29 branch and business awareness communications on AML, Financial Crime and SAR reporting have been delivered in 2020, including a number of communications highlighting vulnerable customer scams. The overall volume of communications reduced in 2020 (from 51 in 2019), partly due to consciously reducing branch impacts during Covid, but also as a result of greater liaison with Area Managers to raise awareness of particular non-conformance issues and scams.

POL00423694

iii. Risk assessment, policies, controls and procedures

23. The Group takes its legal and regulatory responsibilities seriously and consequently has[1]
    - **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
    - **Averse risk appetite** for ligation in relation to Financial Services matters
    - **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
    - **Averse risk appetite** in relation to unethical behaviour by our staff.
24. The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. There were 3 risk exceptions relating to financial crime opened in 2019 and closed in 2020. These were relatively low risk and there was only 1 new risk exception opened in 2020, and this related to Payzone terminals in POL branches *(see Appendix D for details).*
25. All new products and services have been subject to risk assessment before go live, and existing products and services have been subject to annual re-assessment as required. *(see Appendix B for details).*
26. Three Post Office Insurance products that were overdue for assessment in 2019 as the Product Owners returned the Product Information Packs late (Gadget, Motorbike and Pet insurance) were completed in 2020.
27. Policies relating to Financial Crime overall and AML/CTF specifically, have been updated and were approved at the July 2020 Audit and Risk Committee, and published on the Intranet via a One Communication.
28. Both first and second line management have responsibility to ensure that the controls in place work as intended, and the Financial Crime team undertake quarterly assurance checks against the minimum control standards. No controls have been assessed as ineffective, however, there are some areas that are only partially effective and there is on-going work to improve these controls. MI on minimum control standards has been improved and is reported each month. Now that the Fit & Proper system and process has been delivered, quarterly assurance checks for the Fit & Proper Policy Standard will commence in January 2021.
29. We review, investigate and report all instances of non-conformance with AML policies and processes, ensuring corrective action is taken by relevant business owners.
30. Processes within Compliance are robust and up to date, however processes and policies across the business to support these are less mature and continue to require improvement. The planned Compliance Controls Framework will assist with improving business processes and first line compliance with minimum control standards.

iv. Development of new products

31. In October 2020, a new simpler Financial Crime Engagement Tool was launched, to improve engagement between product/project teams and Financial Crime Compliance,

[1] The Risk appetite was agreed by the Post Office Board January 2015

CONFIDENTIAL

POL00423694

and ensure risk assessments are conducted in a timely manner. Initial feedback has been positive.

32. As per the Master Services Agreement between POL and Payzone, some initial work was undertaken to estimate resource requirements for the financial crime assessment of this business. This identified that additional resource would be required to undertake the required activity, as there was insufficient resource within POL and Payzone Compliance teams, and a Fixed Term Contract role is currently being onboarded. There was a delay in recruitment due to budget/funding issues and approval, but these are now resolved and the assessment is expected to be completed by the end of March 2021.

33. The Banking Team are leading on the Community Access to Cash Project (CACP), which aims to ensure communities have access to cash and their bank. They are looking to pilot 9 new Bank Hub locations, which will only offer Banking and Bill Payment services. In addition, there will be a private area which will be shared by Partner Banks so that their representatives can meet with customers. The Banking team continue to explore cash automation and will be trialling 4 self-service deposit machines, 3 of which are expected to be at Bank Hub locations. Whilst these initiatives will increase banking transactions, no new financial crime risks have been identified.

34. There have been no significant products or services launched during 2020 which have changed the regulatory risk landscape for POL.

v. High risk products and services

35. Post Office branch pre-order and on-demand Bureau de Change represents the highest direct risk for POL in terms of AML/CTF and regulatory compliance. Oversight and monitoring enhancements in 2020 include:

    - Improvements to the existing monitoring reports to enable:
        - identification of low value suspicious linked transactions
        - customers/branches who have processed high volumes of declined transactions
        - identification of potentially vulnerable young customers following cases identified at the beginning of March
    - A monthly MI dashboard on monitoring, investigations and SAR activity which is shared with the Travel Money team, together with a monthly compliance meeting to review the MI and discuss any issues identified.

36. There are ongoing issues with the Bureau de Change Credence universe delivered in 2018. Accenture rectified the issue concerning Sanctions whereby customer information was not being pulled through for transactions that declined due to a Sanction match. However, during live testing it was identified that not all transactions processed by a customer are flowing through. There have been ongoing discussions between the Data Centre of Excellence (DCoE) team and Accenture but a solution to rectify has not yet been identified. DCoE believe that this is a defect in Accenture's original design and the original logic to link transactions is incorrect. Weekly calls between the teams to identify a solution are ongoing.

37. During the first Covid lockdown, Financial Crime Compliance supported numerous business projects to adapt to the challenges and ensure that POL was able to support our Postmasters and customers. These included on-boarding Partner Banks to the Payout Now service and simplifying the application process for Drop & Go.

38. Other products that are high risk include:

POL00423694

- Banking cash deposits – We have seen a rise in cash deposits from Partner Banks via POL counters as more customers become aware of the services and more bank branches close. The Covid pandemic and lockdown restrictions throughout 2020 contributed to this and there has been a rise in suspicious activity reports. Financial Crime Compliance have identified third party deposits, money-mules and suspicious deposits by Money Service Business agents. Over the last 12 months there has been a significant rise in investigations and SARs relating to cash deposit services (*see paras 46 & 76*).
- The UK Financial Intelligence Unit (UKFIU) published a report in 2019 calling out the increased number of Post Office cash deposit SARs received, the lack of visibility POL has over bank's customers (meaning that SARs lack detail that would assist Law Enforcement) and stating there were clear indications of money laundering at some POL branches through these services. As a result, Project Admiralty and the SCGC AML Sub-group were established at the end of 2019 to tackle the money laundering risk posed to POL and the banks. This has led to positive changes by some banks to help reduce the risk. This includes reviewing their customer deposit limits, implementing more timely monitoring of POL transactions, and Financial Crime Compliance sharing weekly reports of POL branches investigated for high value deposits.
- Following the Banking Framework Services (BFS) risk assessment in 2019, Financial Crime Compliance have been working with the Banking team to mitigate the risks identified. This included reviewing the BFS agreement wording in relation to the roles and responsibilities of each party. With the aim to make the agreement clearer, new proposed wording was produced by Legal and presented to the SCGC AML Sub Group members in July. Following verbal feedback, amendments were drafted by Legal and circulated in December. The banks have been asked to provide written feedback before 31st January 2021, so that these can be addressed before the proposed wording is formally submitted.
- MoneyGram – As a near real time money transmission service, MoneyGram remains high risk for laundering and scams and there is significant training and awareness activity to help front line staff identify issues. MoneyGram is consistently one of the top three products for which we receive suspicious activity reports by the network each month *(see para 75 & Appendix E)*.
- Gift Cards – Due to the anonymous nature of the product, we continue to see criminal activity which is addressed through training and awareness activity. In response to the Fifth Money Laundering Directive the One4All gift card limit was reduced to £120. Blackhawk (who now own Gift Cards) has approached POL to implement further controls to mitigate the risk of financial crime, and Financial Crime Compliance are supporting the Product team to implement these controls.
- Amazon Vouchers – Between July and September, POL saw an increase in suspicious activity reports relating to Amazon Voucher purchases *(see para 77).* In most reports it is suspected that the customer is potentially vulnerable and has fallen victim to a scam, and in some instances suffered substantial losses. Financial Crime Compliance have been supporting the Product Manager to implement controls to reduce the risk. The Product Manager is a Payzone Bill Payments employee and does not have access to POL information available on the intranet, e.g. Group policies or change procedures. This has caused difficulties in progressing change in a timely manner and meant that we have not yet been able to reduce the risk to our Postmasters and customers.
- Bill Payments Reseller – It was identified this year that an MSB was using POL bill payment service, via Capita, to deposit cash relating to money transmission activity. Deposits were between £10,000 to £20,000 and taking place on a daily basis at one

CONFIDENTIAL

POL00423694

branch. Investigation confirmed the customer was using POL services via a complex bill payment reseller structure - the customer contracted with Zeepay, a client of PIPIT, who in turn are a bill payment reseller with an agreement with Capita. The most recent National Risk Assessment *(see Section E iv.)* again emphasises the risks around complex structures and 'super-agent' money transmission businesses.

POL has an agreement with Capita as a bill payment reseller. Typically, Capita's clients are organisations such as local authorities, charities or utility companies. As per the contract, anything that sits outside the described client type must then be approved by POL. It is believed that POL approved the services for PIPIT back in 2017, however, currently neither party can provide evidence of this, and this was not agreed by Compliance.

Financial Crime Compliance are working with the Product Manager to address this by asking Capita to cease the relationship with PIPIT in relation to POL services, although there are challenges as we cannot enforce Capita to cease the relationship with PIPIT contractually, so are trying to resolve via the commercial relationship.

vi. Customer due diligence

39. POL is required to undertake customer due diligence for directly regulated activity (e.g. Bureau de Change) when:
    - Establishing a business relationship, or
    - Carrying out an occasional transaction with a customer of €15,000 or more, or
    - Money laundering or terrorist financing is suspected

40. For Bureau de Change, the following controls are in place:
    - Horizon restricts single or multiple transactions in the same basket to £10,000 (well below the €15,000 occasional transaction limit).
    - Training and Horizon prompts advise that no business transactions should be undertaken and that customers should not transact more than £10,000 in any 90 day period.
    - Customer details and ID are taken for all transactions of £1,000 and above, and for all transactions settled by card payment. Monitoring is undertaken to identify linked transactions for the same customer in a 90 day period and corrective action is taken as required *(see para 74 re. Bureau de Change investigations).*
    - As part of POLs risk based approach, all transactions of £2000 and over are subject to a real time eKYC, PEPs and Sanctions check, with real time declines of eKYC failures and Sanctions matches.
    - Horizon users are trained to decline transactions and complete a SAR if they suspect money laundering or terrorist financing.

41. PEP matches are monitored post transaction with corrective action taken if necessary. We have identified some matches over the last year, however, we have not identified any concerns as the amounts transacted are very low.

42. Where there is a potential match on a Sanction list the transactions are declined in real time. In 2019/20, there were 4 potential sanction matches and there have been 4 up to P8 YTD 2020/21, which have resulted in further investigation. Following review, none of these potential matches are the actual sanctioned individuals and therefore we have not reported to the Office of Financial Sanctions Implementation (OFSI).

43. In 2019/20, transactions for 42 customers (£217,900) were prevented from breaching the £10k over 90 day Bureau de Change threshold through monitoring activity. P8 YTD 2020/21, transactions for 25 customers (£116,267) have been prevented. We expect this

POL00423694

figure to remain lower compared to last year as the pre-order service was suspended during the majority of Covid lockdown.

44. For all other products and services, POL is not directly responsible for customer due diligence, however, there are some contractual obligations where part of customer due diligence on behalf of the third party client or supplier is undertaken. For example, where POL acts as agent for MoneyGram, we must comply with their policies and processes in relation to recording customer data and identification details. As part of product and service risk assessment work undertaken, the requirement for customer due diligence, PEPs and Sanctions checks is considered, and where appropriate, work is undertaken with the product manager to ensure the right controls are in place.

vii. Reporting suspicious activity

45. All SARs are investigated and, where appropriate, disclosed to the NCA by Financial Crime Compliance. SARs received relating to third party clients are shared with them so that they can conduct an investigation against their own KYC and transaction records.

46. We continue to see an increase of Cash & Valuables in Transit (CViT) drivers raising SARs due to the volume of cash they are collecting. There was a spike in referrals during the first Covid lockdown due to increasing levels of cash being accepted at some branches, which seemed suspicious as most retailers, pubs and restaurants were closed and people were being encouraged to pay by card to help reduce Covid infections. We believe that part of this increase was due to banks opening on reduced hours or temporarily closing during the height of the pandemic, but many are suspicious and we continue to see more reports via CViT.

47. The volume of SARs received increased from an average of 312 per month in 2019/20 to 600 in 2020/21, and in September and October there were over 800. This increase of c.90% was mainly driven by unusual activity identified from Bureau de Change monitoring reports, complex banking investigations completed by Financial Crime Compliance, and SARs received from the Network relating to suspicious bureau activity and banking cash deposits (*See Appendix E: Report on duties of nominated officer for additional information).*

48. The 2 accredited FIO's within Financial Crime Compliance have reviewed, investigated and responded to 145 SARs disclosed by the NCA in 2020, in comparison to 75 in 2019. Some of these related to suspected Bounce Back Loan fraud by persons associated with POL branches. An additional 21 SARs were investigated and responded to by an FIO within Security Operations. This FIO has now left the business and Security Operations will not be recruiting resource with FIO accreditation, therefore Financial Crime Compliance will inherent this workload moving forward, and the impact will be monitored.

viii. Record keeping

49. All record keeping relating to AML/CTF is electronic (all paper SARs and paperwork are scanned and saved electronically) and filed within restricted access folders, with a retention schedule in place. As the team have been working from home due to Covid, a workaround was put in place for paper SARs to ensure these were collected weekly from Future Walk and returned for scanning on to the system and shredding.

50. All reports, risk assessments and supporting documents are filed in the AML Sharepoint site, and a log is maintained to ensure annual review and sign-off.

51. For Bureau de Change, the AML Credence universe maintains all branch on-demand and pre-order Bureau de Change transactions and this is retained for 5 years.

CONFIDENTIAL

52. Financial Crime Compliance investigation cases are managed and recorded via Microsoft Dynamics and maintained confidentially from other Dynamics users in POL. During 2020 there was one incident where users were unknowingly given access to Financial Crime and Security cases. This was quickly escalated, root cause identified, and remedial action taken to resolve it. No material compromises were identified.

53. The Post Office PCI DSS Compliance project will impact how Financial Crime Compliance stores documentation and will alter some key processes and the ability to obtain full card numbers. The new workarounds will impact the time taken to undertake some processes, and will cause some loss of operational efficiency whilst the new systems and practices are embedded. Additionally during branch rollout of the new system, the team will have to access two systems when undertaken certain investigations. Financial Crime Compliance are working with the Project team to ensure requirements are met and understand operational and resource impacts of the new systems.

54. Court Orders & Data Protection Act requests – In 2020, Financial Crime Compliance provided 1 witness statement to the Police and received 17 Data Protection Act requests from Law Enforcement and regulatory bodies relating to fraud and money laundering (consistent with 2019's 16 Data Protection Act requests and 4 witness statements).

ix. Premises Registration

55. Following the HMRC fee increase in 2019, the product team analysed non-profitable branches and permanently removed the product from 3,257 branches. As a result of Covid, discussions were held with HMRC to look at deferring or reducing the annual premises fee due on 1st June 2020 as business volumes had dropped dramatically. A compromise was reached whereby the annual fee was deferred to 1st December 2020, and a further 2,679 branches were temporarily 'paused'. It was agreed that fees for any that were switched back on before 1st December 2020, would also be deferred. The annual fee subsequently paid on 1st December 2020 was £1.656m for 5,512 branches.

56. On 22nd October 2020, it was identified that some de-registered branches were able to transact Travel Money. Subsequent investigations identified that 6 branches completed 25 transactions totalling £6,784.30 between the 1st June 2020 and 28th October 2020. These 6 branches were included in the permanent removal and pausing of HMRC branch registrations at the end of May and should have had their functionality to transact Travel Money "switched off".

57. Historic inconsistencies were subsequently identified between Post Office Master Data System (MDM) and Fujitsu RMD data records, causing the file transmitted to "switch off" the transactions to be unsuccessful for these branches. It was also identified that a further 35 branch records relating to Travel Money transactions were inaccurate but did not result in any transactions.

58. We advised HMRC verbally on 2nd November 2020 of the issue and provided a written report on the 6th November 2020, detailing the anomalies and confirming that the 6 premises impacted were sent for registration on 2nd November 2020, and that the relevant agent (responsible persons) data was still held, they were still considered 'Fit & Proper' and would be supplied in the November monthly HMRC report.

59. HMRC advised on 13th November 2020 that they would be taking no further action or sanction against POL, but confirmed that they will judge all matters on their individual circumstances and therefore any repeated breaches may result in sanctions.

60. Fixes were identified and all the data mismatches were corrected week commencing 9th November 2020, and controls are now in place to prevent future issues; updates to the Fujitsu data records are automated and only transmitted via the strategic Post Office MDM.

POL00423694

61. As a result of this issue, and the data issues called out in paras 65-69 below, Compliance have met with Internal Audit to request that an audit of the data and systems to support HMRC reporting is undertaken when the audit schedule allows in 2021/22.

62. HMRC are expecting to launch a further fee consultation and recognising the regulatory fee burden on POL due to the size of our network, have had two meetings with Post Office to discuss options. HMRC have considered the options and points POL have raised and advised that some suggestions relating to turnover and tiered approaches will be in the consultation. There are currently no agreed timescales for when this will be published.

x. Fit & Proper Test Requirements

63. As in 2019, significant challenges with the Fit & Proper project have continued, with considerable oversight and support required by Compliance. The new system to generate annual declarations, capture data and generate the required reporting for POL internal governance and HMRC agent data provision was further delayed from April to July 2020.

64. The first cohort of redeclarations (500 agents) via the new platform completed successfully and the Declaration Oversight Committee met on the 12th August 2020 to approve all actions. 4 cohorts have now been completed covering redeclarations for 2,954 agents, including all Commercial Partners. No cohort is scheduled in November due to Christmas.

65. There are still a number of ongoing issues which are subject to further investigation and are currently being mitigated by manual processes:

- Issues with Power BI reports to produce the Revoke Report (to switch off bureau transactions for non-compliant agents) and the monthly HMRC Reporting.
- Ongoing data refresh issues preventing the responsibility being passed to the BAU teams (F&P Ops and Branch Insights Team)
- People data extraction from the Financial Assessment (formally Electronic Business Plan) is more cumbersome and labour intensive than first thought due to missing data on the report
- Legal Status discrepancies are being flushed out by the redeclarations – these should have been resolved by the project team when the first declarations were received. These are being resolved but it is causing unforeseen resource pressure in the F&P Ops, Contracts and Onboarding teams
- Cohort rebalancing required in Q4 will require some Postmasters to redeclare under a year since their last declaration

66. A further release was needed in November to ensure the inclusion of 'paused' and MoneyGram only branches, as the decision to permanently and temporarily de-register branches in May was too late for design amendments to the F&P system being delivered. Some issues were identified with the second release, and data matching required for the migration then identified an issue with CFS data feeds not working during a 'non-cohort' month. This was corrected in time for the HMRC agent data return in November.

67. Self-serve declarations for Sole Traders via Branch Hub are being developed by Accenture for delivery in January 2021 in time for the next cohort. This will allow straightforward 'no change' redeclarations to be completed via this simplified route.

68. The F&P Ops team transferred into the Postmaster Effectiveness function as part of the recent restructure and there will be a new F&P Ops lead. With the ongoing reporting,

CONFIDENTIAL

POL00423694

data, system and process issues still being investigated and resolved, a change in management oversight at this stage presents a risk, as critical 'corporate memory' and understanding of the system may be lost.

69. There have continued to be challenges in keeping direct employee F&P records up to date. Following the removal of the role previously overseeing the work in February 2020, responsibility transferred back to Financial Crime Compliance. Working with HR a new flag has been created in Success Factors against the position codes for impacted roles, generating fortnightly reporting to the MLRO of any changes. This ensures impacted individuals apply for the test, and those leaving impacted roles/Post Office are removed from HMRC records. However, the most recent OE changes have made it difficult to keep this up to date as individuals leave the business and role titles/responsibilities and line management changes have occurred. Financial Crime Compliance is working closely with HR to resolve current discrepancies.

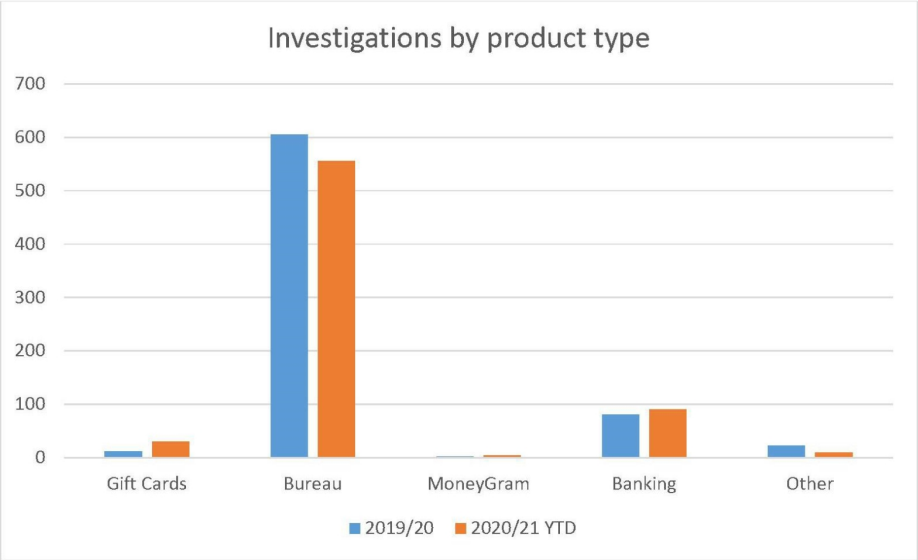
70. Further work will be required throughout 2021 to provide compliance assurance.

D. Investigations and Incidents

71. There were 689 investigations up to P8 2020/21 (an average of 86 per month), compared to 727 for the whole of 2019/20 (an average of 61 per month). Bureau de Change investigations up to P8 2020/21 are almost at the level for the whole of 2019/20 and it is expected this level will continue as enhanced monitoring reports are developed and implemented. Monthly meetings are held with the Travel Money team to review MI and trends, and determine if further system changes or controls are required in Horizon to reduce manual investigation activity.

72. Banking investigation volumes to P8 have exceeded the total seen for the whole of 2019/20, mainly due to increased banking cash deposits due to Covid, bank closures and reduced opening hours. Since March 2020, a growing trend was identified with MSBs depositing significantly high volumes of suspicious cash over our counters *(see para 76).*

73. The graph below shows the investigations undertaken in 2019/20 and up to P8 2020/21 and is split out by the high risk products:



CONFIDENTIAL

POL00423694

74. Bureau de Change (volume and value of branch transactions 2019/20 5.96m & £1.38bn, and to P8 2020/21 914k & £241m).

- Due to Covid, transactions are significantly down compared to last year, although up to P8 YTD 2020/21 there have been 556 investigations reflecting criminal and customer behaviour changes. These related to branch non-conformance, money laundering and confirmed card fraud.
- Refinement of monitoring reports has led to an increase in the identification of potential vulnerable customers and helped highlight customers travelling to multiple branches to purchase currency:
  - A high number of potentially linked customers travelled excessive distances from their home addresses undertaking multiple purchases of foreign currency, which continued during November lockdown. This was referred to the NECC, due to suspicions about links to Modern Slavery/Human Trafficking. The majority of the customers ceased transacting following direct escalation to Regional and Relationship Managers and contact with branches.
  - An emerging pattern was identified, potentially linked to County Lines drug dealing, involving several young males and females (16-22 years old) completing transactions at multiple POL branches. A branch focus article was issued to the Network and information shared with Regional and Area Managers to raise awareness. The card information was shared directly with the card issuing bank, and the information was referred to the NECC.
- All non-conformance is escalated to the Area Managers and Contracts teams, and there have been a number of Area Manager visits and conversations in order to prevent any further breaches. Up to P8 2020, 69 incidents were escalated to these teams.
- Via Microsoft Dynamics 365, a record is maintained of mitigation undertaken for each case. Up to P8 2020/21 volumes of activities needed have increased significantly:
  - 1480 Branch phone calls (1602 for whole year 2019/20)
  - 287 Text blasts (121 for whole year 2019/20)
- Multiple examples have been identified in 2020 of customers sharing cards, travelling to transact, and purchasing lower values possibly to avoid card limits or to obtain cash advances. Where possible, transactional bureau information is shared with the card issuing banks to aid their investigations. These bank referrals have helped limit further breaches.

75. MoneyGram (volume and value 19/20: send transactions 2.5m & £561m, receive transactions 340k & £99m. Volume and value to P8 19/20: send transactions 1.6m & £416m, receive transactions 176k & £53m).

- Monthly meetings are held with the MoneyGram compliance team to review any issues.
- During 2020, the Network has reported vulnerable customers sending money to various South American countries and India. Trends have been identified including fraudsters targeting vulnerable customers posing as Microsoft requesting access to home computers and HMRC demanding tax payments. All reports have been escalated to MoneyGram via the fortnightly SAR update and urgently via phone if required.
- Concerns were raised directly to the MoneyGram Compliance Team regarding individuals sending high values to Romania and Albania, using one branch to transact. In some instances, these customers all claimed to live on the same streets. This resulted

CONFIDENTIAL

POL00423694

in the suspension of the MoneyGram service at the branch and after review the branch send limit was reduced indefinitely.

- MoneyGram have identified 52 potential branch non-conformance issues up to P8 2020/21 (107 were identified in 2019/20). MoneyGram has conducted a review at each branch, either in person or over the phone, discussing the failings and providing further training where required. Prior to each review, Financial Crime Compliance complete a check of each branch to confirm whether any other concerns exist.

76. Banking Framework Services Cash Deposits (Volume and value 2019/20: 41.3m & £22.1bn. Volume and value up to P8 2020/21: 25.5m & £12.5bn).

- There were 90 investigations totalling c.£198m relating to suspicious high volume/ value banking cash deposits up to P8 2020/21. This is compared to c.£98m across 80 investigations in the whole of 2019/20.
- The examples below have been identified from intelligence received and SARs raised by branches, cash centre staff, Area Managers and third parties:
    - There has been a significant increase in large cash deposits being made by MSBs operating as sub-agents for Money Transfer Services across the UK, with the majority in East London. At one branch in East London, c.£68.5m was deposited between 12/02/2020 and 16/11/20 onto c.40 different bank cards and into multiple different bank accounts which we understand all belong to MSBs. c.£9.9m has also been deposited at a branch less than half a mile away with some individuals depositing at both branches. Following referral by Financial Crime Compliance, one bank has exited two MSB relationships, and one bank is writing to their MSB customers to advise that they must pay in via the bank and not POL so they can closely monitor activity.
    - Intel from one bank identified, high value cash deposits being made onto multiple banks cards. Between February 2020 and October 2020, c.£17.6m was deposited at 148 different POL branches, predominately in the South, South West and South East of London. Following law enforcement engagement, an individual was arrested and pleaded guilty to money laundering offences
    - SARs were received from two branches in South East London and Kent raising concerns that customers were depositing large volumes and values of cash into two different bank accounts. It was identified that deposits were taking place at 58 POL branches totalling c.£3m between 03/08/20 and 24/09/20. Working closely with the banks these accounts were exited and the activity subsequently stopped. Area Managers were asked to speak to the impacted branches to ensure deposits are refused if these customers return.
    - A branch raised a SAR concerning high values of cash being deposited into a Hydroponics business. Investigation identified four additional cards depositing at 4 other branches and between September 2019 and 23rd March 2020, c.£4m was deposited in total. Branches advised that the notes often smelt of cannabis and the individuals provided contradictory information regarding their nature of business, they also often deposited Scottish notes which was unusual for their area. After liaising with law enforcement and the banks involved, a number of individuals have been arrested on suspicion of drugs and money laundering offences.

77. Amazon Gift Vouchers – SARs received in the second half of 2020 highlighted customers duped into purchasing vouchers and providing the voucher code to fraudsters over the phone. Often the fraudster telephones the customer alleging to be from HMRC and

POL00423694

advising that they owe large amounts of tax which has to be paid that day otherwise they will be arrested for tax fraud. The customer is told that the only way they can settle the debt is by purchasing Amazon gift vouchers. In one example, an elderly customer visited a branch on three occasions and purchased £14,500 worth of vouchers with cash withdrawn from his bank, on each occasion he advised that he was buying these for friends and family. The branch reported this to Grapevine and were advised to initiate Banking Protocol should he return. He returned the following day and attempted to purchase a further £6,600 worth of vouchers, Police were called and while the customer was waiting to be served, he received a call from the fraudster asking if the transaction had been completed. When the Police questioned the customer, he finally admitted that he was buying the vouchers and providing their code numbers to someone claiming to be from HMRC, as he had to pay a tax demand or he would be arrested. Further checks carried out identified he had visited two other branches and purchased £30,000 in total.

Multiple nationwide communications to the network have been issued and awareness raised via the weekly Retail Network. Financial Crime Compliance are working with the product team to implement additional controls to reduce the risk *(see para 38).*

78. Card Fraud over POL counters – Between 1st January 2020 and 30th November 2020 there were 2345 fraudulent card transactions processed totalling £202,592.81. In the same period last year there were 2198 totalling £250,549.25. The majority of fraudulent transactions over £100 continue to relate to Gift Card purchases. Investigations are carried out where a particular branch is being targeted, or when high value amounts have been purchased. Branch communications have been delivered and SARs raised where required.

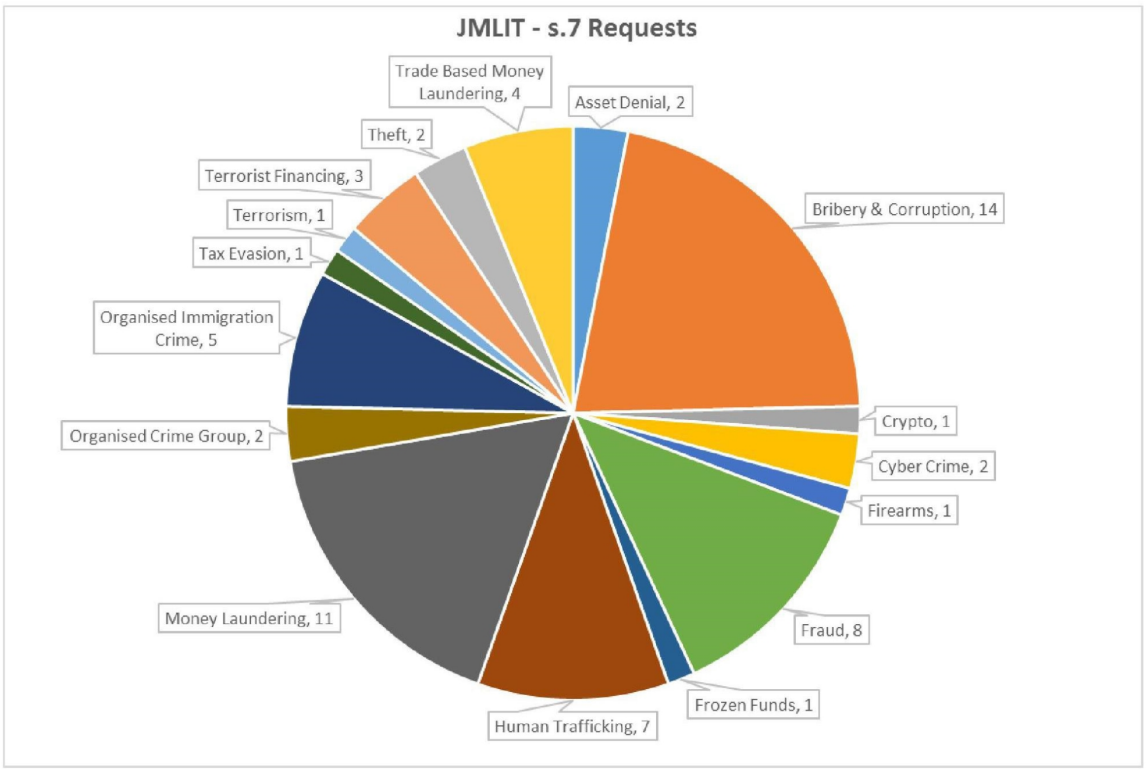
79. The volume of JMLIT[2] s.7[3] requests received to P8 2020/21 has reduced in comparison to last year due to the impact of Covid on law enforcement activity, however, this remains high in comparison to previous years:

- s.7's requests received - 65 (87 during previous year up to P8)
- Number of searchable subjects included in the requests – 832 (1060 during previous year up to P8)
- Number of subjects identified in POL data – 18 (36 during previous year up to P8)
- More investigations have focussed on foreign Bribery & Corruption, and money laundering through offshore businesses with fewer investigations linked to Human Trafficking and Modern Slavery. As a result, POL have provided half the s.7 returns in comparison to the same period last year due to a smaller footprint recorded against POL products and services.
- The chart below shows the underlying issues for each s.7 request received:

[2] Joint Money Laundering Intelligence Taskforce – Post Office is a member of the Operations Working Group
[3] Under section 7 of the Crime and Courts Act 2013, the NCA is empowered to request information for the purposes of exercising any NCA function, responses to these data requests are a key activity for JMLIT members.

CONFIDENTIAL

POL00423694



E. External Threats/Landscape

i. Business areas

80. There have been no significant changes to the regulatory landscape during 2020 as a result of changes in the Post Office business model.

ii. The impact of Covid-19

81. Covid has had a significant impact on the Financial Crime landscape, and there has been a general increase in frauds, scams and changes in Organised Criminal Gang's (OCGs) activities across the financial services industry both in the UK and overseas.

82. An increase in financial crime has been reported throughout 2020 due, with the NECC reporting that they expected to see increases as typologies adapted to the new restrictions. By April, Action Fraud had reported that 862 reports had been received relating to COVID with losses totalling over £2m.

83. The Fraud Advisory Panel reported that the following Covid fraud risks had been identified:

- Phishing emails and letters (especially via Zoom and Microsoft 365).
- Fraudulent/fictitious investment opportunities advertised via social media platforms.
- Fraudulent coronavirus insurance adverts.
- Fake fines claiming the individual has broken lockdown rules.
- Business impersonation (e.g. requests for employees to update their bank details).
- Companies advertised on eBay potentially involved in Bounce Back Loan fraud.

CONFIDENTIAL

POL00423694

- Financial services firms seeing widespread evidence of government grants, particularly Bounce Back Loans, being exploited with a high level of sophistication by both OCGs and individuals.
- Fraudsters paying young adults for their personal details which are then used to form companies, open bank accounts, and register for grants.

84. The NECC with support from UK Finance, established a Covid Fusion Cell at the beginning of April, which ran until December 2020. It included banks, Post Office, UKF, CIFAS, Insurance, IFB and British Telecom plus the public sector (NECC, HMRC, COLP, MPS) to share information to identify changes in the economic crime threat and criminal behaviour during the restrictions and target where action could be taken against criminal behaviour, and identify alerts/typologies/communications to be issued cross-sector to help prevent economic crime.

85. Post Office has seen an unprecedented increase in SAR reporting and investigations *(see paras 47 and Section D),* and has also identified a number of existing or new agents via SAR disclosures and agent applications that may have mis-used, or attempted to mis-use Bounce Back Loan and other Government backed Covid support. We have also seen a rise in vulnerable customer scams and frauds and a number of activities have been undertaken to address these issues *(see paras 38 & 74).* Business Plans Analysts referred potential mis-use of BBL funds in new Postmaster applications to Financial Crime Compliance who sought guidance from the British Business Bank. This guidance was used to establish and issue guidelines for the Agent On-boarding teams and Business Plans Analysts.

iii. Fifth Anti Money Laundering Directive

86. The Fifth Money Laundering Directive (5MLD) was implemented in the UK on 10th January via the Money Laundering and Terrorist Financing (Amendment) Regulations 2019. There was limited impact to Post Office in respect of the new regulations:

- Enhanced Due Diligence was expanded to include business relationships or transactions involving high-risk third countries and required enhanced monitoring. MoneyGram implemented changes to its processes for sending and receiving money involving high-risk countries and these changes were communicated to branches.
- Electronic Money amendments reduced thresholds for anonymous pre-paid cards. GiftCard limits had already been reduced to a maximum £120
- Risk assessments must be completed prior to the launch or use of new products, business practices and delivery mechanisms. This is an existing minimum control standard in POL policies, but first line adherence is inconsistent and steps have been taken to address via training and awareness.

iv. National Risk Assessment (NRA) of Money Laundering and Terrorist Financing 2020

87. The third NRA was published on 17th December 2020. It concludes that it remains difficult to quantify the scale of the money laundering threat to the UK, but it is likely that levels have increased since 2017 and estimates that serious and organised crime costs the UK economy £37billion a year.

88. Key findings include:

- Traditional high-risk areas of money laundering remain, including financial services, money service businesses, and cash. However, new methods continue to emerge within these, as criminals adapt to increased restrictions and exploit vulnerabilities in different sectors and emerging technology.

POL00423694

- Retail banking services continue to be assessed as high risk of being abused for money laundering. Criminals continue to target retail bank accounts to facilitate the rapid transfer and layering of criminal proceeds. Those that accept cash deposits face the highest risk.
- Cash-based money laundering is still heavily characterised by the use of cash intensive businesses to disguise criminal sources of wealth, or by smuggling large amounts out of the UK. However, an increase in the abuse of cash-related services has been noted, such as cash deposit services in Post Offices, and the use of cash couriers and CViT companies. This is alongside continued abuse of legitimate UK services, such as money transmission and retail banking.
- Currency exchange is stated to be usually lower risk than money transmission services. This is due to the large volume of money that can transfer across borders and the vulnerabilities associated with money transmission business reliance on a complex network of agents and sub-agents to deliver their services enhancing the risk of exploitation by criminals.
- It is estimated that at the end of 2019, there were around 4,800 criminal groups in the UK, comprising approximately 37,000 associated nominals.
- NCA assesses it is likely fraud in the UK is increasing, with a considerable rise in reported losses
- The threat to the UK from terrorism was raised to 'severe' (an attack is highly likely) on 3 November 2020.
- The size of the illicit drugs market in the UK in 2018 was estimated to be £5.3 billion, but recent research into specific drugs suggests the actual figure is much higher.
- Detections of migrants attempting to enter the UK illegally have increased, and the criminals facilitating them continue to use high-risk smuggling methods.

v. National Economic Crime Centre – Public/Private Initiatives

89. Following the establishment of the NECC in 2019, they are improving public-private partnership by bringing together all public-private activity under one governance forum through the creation of a new NECC Public Private Operational Board (PPOB). The working groups within JMLIT have been reduced to 3 (Fraud, Money Laundering & Terrorist Financing), with the agreement that 'pop-up' groups will be established where necessary to tackle particular threat (e.g. the Covid Fusion cell set up in April and Project Admiralty set up end 2019 to co-ordinate responses to the increased threat of cash deposits over POL counters).

90. Since March, the JMLIT Operational Working Group has not been able to meet, as there is not a safe alternative to the physical weekly meetings at the NCA, but matters have been dealt with via secure correspondence and some group and bi-lateral conference calls.

91. Work has been undertaken during the year, and supported by Post Office, on the Public Private Threat Update relating to MSBs and the 3rd National Risk Assessment on Money Laundering and Terrorist Financing, published in December *(see section i.v. above)*.

92. In the Autumn, HMT in issued a consultation on the proposed Economic Crime Levy. The paper indicated that their preferred option is to have a revenue based levy with some exemptions for small businesses where it is not cost effective to gather the levy. We have put forward a position that as all POL regulatory revenue is derived via payment of dividend and commission from FRES, who are also regulated and subject to the levy, this would effectively be a 'double-levy' and therefore POL revenue should be exempt. We are unlikely to see a response to the consultation, and the draft legislation until the new year.

POL00423694

vi. FCA penalty for Anti-Money Laundering failures

93. In June 2020, FCA fined Commerzbank AG (London Branch) £37.8m for failing to put adequate AML systems and controls in place between 2012 and 2017. Commerzbank was aware of these weaknesses, which FCA had previously raised with them, and had failed to take reasonable and effective steps to fix it.

vii. Sanctions Policy after 31st December 2020

94. When the UK's transition period after Brexit comes to an end, EU sanctions will no longer apply in the UK. The UK sanctions regime will come into force, from 11pm on 31st December 2020, under the Sanctions and Anti-Money Laundering Act 2018 (Sanctions Act). There will be no gaps in implementing existing sanctions regimes after the transition period. Some EU sanctions regimes may not be addressed through regulations under the Sanctions Act by 31 December 2020, but these will continue as retained EU law under the EU (Withdrawal) Act 2018. The government will implement UN sanctions in UK domestic law after the transition period.

viii. Other external threats

95. In February 2020, the NCA published an Amber Alert to warn registered money service businesses that serious organised crime networks were specifically targeting the sector for its weaknesses in detecting dirty cash. During lockdown Post Office identified an increase in independent MSBs (or independent retailers registered as agents of larger companies, such as Ria) depositing their cash proceeds over POL counters.

96. Romance and dating fraud: Action Fraud has seen a 26% increase in reports in 2020, with the average victim of romance fraud losing just over £10,000. Losses reported by victims between August 2019 and August 2020 totalled £66,335,239. Criminals are targeting victims via dating sites and are then encouraging them to send money via money transfer companies such as MoneyGram. City of London Police have been working with money transfer companies to block suspicious transfers.

F. Conclusions and Recommendations

97. The regulatory environment continues to pose a challenge, with increased regulatory and legislative focus on money laundering and terrorist financing. The 2020 NRA published in December 2020 demonstrates risks remain high, particularly in relation to cash based services, and calls out in the executive summary the risks associated with banking cash deposits over POL counters. We expect HMT to introduce an Economic Crime Levy in 2021, and this will increase the regulatory fee burden for POL and increase scrutiny from law enforcement and supervisors as funding from the levy is applied to target money laundering risks.

98. Covid has had a significant impact on the Financial Crime landscape, and there has been a general increase in frauds, scams and changes in Organised Criminal Gang's (OCGs) activities across industry. There has been an increase in scams relating to vulnerable customers and particularly linked to Amazon vouchers and we are supporting work by the product team to enhance controls. We have seen examples of suspicions activity in POL related to potential misuse of BBL by prospective agents, and have worked with the Agent On-boarding teams to implement controls. The volume of SARs have doubled and investigations risen by a third in the last 12 months, leading to the recruitment in October of an additional PO grade into the Financial Crime Compliance team funded until the end of 2020/21. There is no indication that volumes are reducing, and in September and October SAR volumes were almost treble the average seen in 2019, therefore this resource will need to be fully funded for 2021/22.

POL00423694

99. Significant focus has been given over the last 12 months by the NECC and Post Office in addressing the risks relating to cash deposit services, but as more banks close and more bank customers use Post Office the risks continue to grow, and Post Office needs to be able to demonstrate that it is both aware of the risks, and has controls in place to manage them. In 2020 up to P8 there have been 90 investigations involving c. £198m suspicious cash deposits – the amount of suspicious deposits is more than double that for the whole of 2019. We have continued to support the NECC Project Admiralty established to tackle the cash deposit threat over POL counters, and at the December meeting, 4 participating banks confirmed that they have improved their account monitoring relating to these transactions. We also established a BFS AML Sub Group in February to highlight and discuss the issues with the banks, and improvements to the BFS agreement to more explicitly call out the responsibilities of POL and the banks in relation to regulatory matters have been drafted and submitted for review and comment by the end of January 2021.

100. Cash deposit values seen in 2020 relating to Money Transmission Businesses have highlighted an unforeseen issue with businesses that deposit excessive volumes of cash through a single location. Whilst actions have been taken to address the physical security risks associated with these, further consideration is needed to tackle the money laundering placement risks associated with accepting high value cash deposits from high risk businesses. A robust solution needs to be identified and put in place to ensure that Post Office can demonstrate to regulators, if called upon to do so, that sufficient controls are in place.

101. The HMRC supervisor who had overseen Post Office regulated activity since 2015 retired in May 2020 following handover to a new supervisor. A joint meeting was held in February to demonstrate the controls that Post Office has in place in respect of Bureau de Change. Unfortunately, the new supervisor secured a new role in the summer and a further supervisor was appointed in August. An initial virtual meeting has been held, but due to continuing Covid restrictions, HMRC are not undertaking any supervisory visits or meetings, and it is unclear what level of scrutiny we may see in 2021. We are also expecting a further consultation on HMRC's fee structure in 2021.

102. Training is a key AML control for Post Office. There have been some instances of poor/late completion of mandatory training by employees and contractors, but these issues are being addressed with the assistance of Learning & Development. Completion will be monitored more closely in 2021. We still see instances where SARs should have been raised by branches, and more awareness raising via Area Managers is planned. The resource responsible for training, awareness and communications was removed in November 2020 as a result of OE, and whilst the Communications Team will still support communication activity, the work to support training content will have to be undertaken primarily by Financial Crime Compliance moving forward, and this may impact the ability to further enhance training.

103. Both first and second line management have responsibility to ensure that the controls in place work as intended. Quarterly assurance checks against the policy minimum control standards by Financial Crime Compliance evidence that a number of first line controls are only partially effective. Processes within Compliance are robust and up to date, however processes and policies across the business to support these are less mature and the planned activity in 2021 by Compliance on the Controls Framework should help improve first line understanding and application of their responsibilities.

104. Products and services provided by Post Office are broadly in line with the risk appetites set by the Board and there has been a general improvement in residual risk over the last 12 months. The introduction of the new Financial Crime engagement tool simplifies the initial

POL00423694

assessment of new products and services, and work is ongoing to improve the full risk assessment process. There have been delays starting the Payzone risk assessment due to resourcing and funding challenges, but these were resolved in Q3, and recruitment of a fixed term contract Financial Crime Manager to complete the work is underway, with a target for delivery of the assessment by the end of the financial year.

105. A SAR received from one branch identified a complex trading structure with links to overseas money transmission companies via the Bill Payment Services, exposing an issue relating to product understanding of exactly what types of businesses are serviced under re-seller contracts. The controls relating to these contracts will be reviewed as part of the Payzone and Bill Payments reviews in 2021.

106. The accredited FIO within Security Operations who assisted with the review of SAR disclosures relating to possible Post Office employees and postmasters has left the business and the replacement resource will not have FIO accreditation. Financial Crime Compliance will have to absorb this additional workload moving forward.

107. The POL PCI DSS Compliance project will impact Financial Crime Compliance adding additional time to some activity, as card data will need to be accessed, processed and stored in a 'clean room' environment. Additionally, during the rollout period, both the existing and new systems will need to be accessed when undertaking investigation work. We are working closely with the project team and have called out that additional PO resource may be needed to support this transition period.

108. As in 2019, there have continued to be significant challenges with the Fit & Proper project with considerable oversight and support required. The new system for generating annual declarations, capturing data and generating the required reporting for Post Office internal governance and HMRC agent data provision was delivered in July 2020, but there are on-going teething issues (resulting on one occasion in requesting from HMRC approval of a late submission of monthly data), and the F&P team has moved under a new team leader as a result of OE, therefore the knowledge and expertise built up by the original team leader during the last 6 months will be lost. Further oversight and work will be required to ensure compliance in 2021.

109. Despite improvements relating to direct employee F&P processes implemented in the first half of 2020, the most recent OE changes have made it difficult to keep this up to date as individuals leave the business and role titles/responsibilities and line management changes have occurred. Financial Crime Compliance is working closely with HR to resolve current discrepancies and implement more robust controls.

110. Further work has been undertaken to improve and implement the Bureau de Change monitoring reports. This has led to an increase in cases despite the reduction in overall transaction volumes caused by Covid. The new reports have enabled the identification of potential vulnerable customers and highlighted customers travelling to multiple branches to purchase currency, further evidencing the improvements in monitoring controls since the HMRC audit in 2016. The monthly meetings now held with the Travel Money team ensure they have direct oversight of the activities to support their produce, and also ensure Financial Crime Compliance are kept up to date with any product changes or developments.

CONFIDENTIAL

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Project Assurance – Post Office Section IRRELEVANT IRRELEVANT	**Meeting Date:**	12 January 2021
Author(s):	David Scothern, Programme Manager (Interim) Maxine Cross, Rewards and Pension Director Laurence O'Neill, Senior Legal Counsel, HR & IR	**Sponsor:**	Lisa Cherry, Group Chief People Officer

Input Sought: Noting

The Risk & Compliance Committee (RCC) is asked to note:

- the progress on Project Assurance, the programme of work to resolve the IRRELEVANT IRRELEVANT;
- the progress against actions from the previous Audit, Risk & Compliance (ARC); and
- the continued reporting/dialogue with IRRELEVANT

for onward submission to the ARC.

8.1

Previous Governance Oversight

- 22 September 2020 ARC endorsed the earlier decision of RCC to report the IRRELEVANT IRRELEVANT which was done on 9 October 2020 and acknowledged by them on 14 October 2020.
- ARC recommended that the matter be escalated to Board so that they have visibility.
- Board update of 27 October 2020 following GE update of 14 October 2020 to inform of progress towards the resolution of the IRRELEVANT
- The actions from the last meeting were to ensure ARC had sight of IRRELEVANT arising and the controls in place to deal with them.
- Actions to quantify the IRRELEVANT and the timescale will be discussed in more detail at GE/Board meetings

Executive Summary

In July 2020 ARC was advised of IRRELEVANT

IRRELEVANT

Since the last report to the Board on 27 October 2020 a Project Steering Group has been convened with terms of reference to oversee the IRRELEVANT The group has met twice and includes the sponsor (Lisa Cherry) and three other GE members (Al Cameron (Group Chief Finance Officer), Richard Taylor (Group Corporate Affairs, Brand and Communications Director), Ben Foat (Group General Counsel))

IRRELEVANT was sent to POL actuaries, Willis Towers Watson, on 26 November 2020 for review and on to the IRRELEVANT shortly afterwards., IRRELEVANT required by the IRRELEVANT only, was sent on 22nd December 2020.

The review by POLs actuaries of the IRRELEVANT is due to complete in January 2021. The data set is all of the changes for all IRRELEVANT from April 2014. Actuaries for

Confidential

POL00423694

the IRRELEVANT will then analyse this data to identify any changes to 2017 IRRELEVANT data and to inform the approach to IRRELEVANT Once this analysis has been completed it will be presented to the IRRELEVANT (expected on 23rd March 2021). We expect the IRRELEVANT to engage with POL after this point to seek a IRRELEVANT POL may wish to pre-empt this be setting out its position on IRRELEVANT

The IRRELEVANT has indicated that the IRRELEVANT work will complete in September and now expects to make the IRRELEVANT as late as "early" 2022 – which is close to the 1 April 2022 deadline to IRRELEVANT The plan is based on the 2017 IRRELEVANT data being accurate and the IRRELEVANT being able to IRRELEVANT IRRELEVANT The IRRELEVANT is IRRELEVANT the IRRELEVANT and expects to complete this IRRELEVANT in March 2021.

The Steering Group has challenged the project to work with the IRRELEVANT to find way of accelerating this timeline and ensure that the IRRELEVANT IRRELEVANT At the very least, we should seek to arrive at the position where the IRRELEVANT understands that POL will IRRELEVANT IRRELEVANT The Steering Group also wished to see interim communications plans that satisfies both the IRRELEVANT desire not to give too much detail until the full picture (including IRRELEVANT) is understood and the IRRELEVANT

We have reported the issue to IRRELEVANT initially on 9 October 2020. IRRELEVANT is being kept regularly informed of progress and is aware that data was sent to the IRRELEVANT on 30th November. We committed to a further update by 31 March 2021 or when the IRRELEVANT has finished its analysis whichever is the sooner.

8.1

Questions addressed

A. Why has the investigation taken this long to date?
B. Have the key impacts changed since the previous report to ARC?
C. What are the current risks and mitigations?
D. What action have been taken since the matter was last before the Board on 27th October?
E. What are the next steps and timelines?

Report

A. Why has the investigation taken this long to date?

1. The investigation stage has taken until now to complete for a number of reasons, the timeline of which is summarised in Appendix 1:
   - IRRELEVANT
   - IRRELEVANT
   - IRRELEVANT IRRELEVANT The data set

Confidential

POL00423694

runs to over 200,000 lines of data sources from two system (IRRELEVANT) and has had to be IRRELEVANT IRRELEVANT

- Data / Calculation validation – During and following the IRRELEVANT of the data this has then undergone independent IRRELEVANT by both our Corporate actuaries as well as input from the IRRELEVANT actuaries. The data has now been passed formally to the IRRELEVANT actuaries for their phase of the assessment.

B. Have the key impacts changed since the previous report to the ARC?

2. The types of IRRELEVANT and the areas of impact remains unchanged. The magnitude of these impacts has changed as described below:

3.

4. IRRELEVANT

5.

8.1

Confidential

POL00423694

6. IRRELEVANT

C. What are the current risks and mitigations?

7. The execution risk, should there be significant changes to the IRRELEVANT data that was the basis for the IRRELEVANT and the terms for the IRRELEVANT is managed by the IRRELEVANT

8. The major risks to POL, the financial and reputational risks stemming from the IRRELEVANT are discussed below:

9. **Financial Risk:** Generally speaking, the costs of IRRELEVANT will be borne by the IRRELEVANT itself. However, the IRRELEVANT has indicated verbally that it expects IRRELEVANT

IRRELEVANT

IRRELEVANT

10. **Reputational Risk**: POL reported to IRRELEVANT on 9 October 2020 and has been keeping the IRRELEVANT updated with progress. We committed to a further update by 31 March 2021 or when the IRRELEVANT has finished its analysis whichever is the sooner. Our interactions with IRRELEVANT to date reflect our initial view that, provided we demonstrated that we had a proper IRRELEVANT plan in place, IRRELEVANT would be content to take a hands-off approach.

We also have reactive communications in place to deal with any leaks.

8.1

POL00423694

To date we have managed to align communications from the IRRELEVANT The messaging was high level and avoided any discussion of IRRELEVANT We now wish to move to more detailed communications to pave the way for IRRELEVANT to those thinking about IRRELEVANT We would expect the IRRELEVANT to be supportive of this – it would enable them to be open with their IRRELEVANT about the IRRELEVANT but the IRRELEVANT will be very reluctant to make such a move. There is a meeting to discuss this in January 2021.

D. What actions have been taken since the matter was last before the Board on 27th October?

11. The following actions have been taken since 27th October:
    - An update was to IRRELEVANT on 4 December 2020 advised that data had been sent to the IRRELEVANT
    - IRRELEVANT was provided to WTW on 26 November 2020 and shortly afterwards to the IRRELEVANT to assist with their preparation for IRRELEVANT
    - The IRRELEVANT has produced a high-level end-end plan

E. What are the next steps and timelines?

- January
    - WTW complete their review of IRRELEVANT
    - POL and IRRELEVANT finalise and sign a IRRELEVANT IRRELEVANT
- February/March
    - IRRELEVANT WTW confirms the IRRELEVANT
    - IRRELEVANT validates the plan for IRRELEVANT
    - Date is confirmed for POL to start working in accordance with new "future state" processes (expected to be April)
    - IRRELEVANT reports to the Board on the impact of the IRRELEVANT

8.1

POL00423694

Appendix 1

A summary of the key points in the timeline is as follows:

- **February 2020:** IRRELEVANT
- **March 2020:** IRRELEVANT
- **April 2020:** POL appointed professional assistance to help investigate and resolve the IRRELEVANT IRRELEVANT
- **May – July:** Data gathering and build of IRRELEVANT
- **August 2020:** Legal advisors for the IRRELEVANT and POL agree on IRRELEVANT IRRELEVANT
- **September 2020:** Data finalised and constructed IRRELEVANT
- **October 2020:** Data is sent for review to actuaries representing POL and the IRRELEVANT IRRELEVANT
- **November 2020:** A IRRELEVANT data set is sent to the actuaries who expect to keep their review in January
- **December 2020:** IRRELEVANT data sent to the IRRELEVANT team

This complexity on the POL side will be mirrored on the IRRELEVANT side as IRRELEVANT IRRELEVANT

8.1

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Success Factors Update	**Meeting Date:**	12 January 2021
Author:	Helen Rhodes, People Shared Services Centre Director	**Sponsor:**	Lisa Cherry, Chief People Officer

Input Sought: Noting

The Risk & Compliance Committee (RCC) is asked to note the progress of the process improvement work ongoing in People Shared Service Centre (PSSC) for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

- The SuccessFactors (SF) Response Paper was presented in the September 2020 ARC meeting. It was agreed that SF should be utilised to its full potential and gave the go ahead for process/ system enhancement work in PSSC.
- The purpose of the process and system enhancement work in PSSC is to ensure best use from SF and to ensure that processes become more efficient whilst maximising the use of automation, mitigating risks and assuring compliance.

8.2

Executive Summary

The Process Improvement project within PSSC began in September 2020. The project identified 202 processes and sub-processes within the service which all needed to be documented, reviewed and, where possible, improved.

By 31st December 2020, 74 processes have been fully reviewed and documented. 38 improvements (including 'work in progress' tickets) have been made to SF configuration through the small changes process with current suppliers, leading to no additional spend for improvements. The introduction of Process Improvement specialists and Service Centre expertise has increased rigour and control to the development of efficient processes and BAU operations of SF, leading to a culture of continuous improvement,

Through the Organisational Effectiveness programme and as a result of process efficiencies, it has been identified that PSSC is able to reduce by 6 roles in Tranche 2.

Further work has also taken place to address the recommendations in the Deloitte Report. As a result, it has been identified that along with the process improvement work, Service Now HR module could be introduced as a complementary and integrated technology to SF. This will be a key technical enabler for the PSSC, providing consistency of approach to customers, full audit trails and the ability to report key service measures. This piece of work is currently being scoped, as the SNOW has been confirmed as fit for purpose for our needs. A business case is being developed in order to articulate the full cost of the change to ensure benefits delivered (e.g. change resources, related process change and tool roll out). Target submission date is the end of January 2021. This will be managed and reported on via the OE Portfolio and in alignment with TOM activities.

Strictly Confidential

POL00423694

Questions addressed

1. What progress on process improvement has been made since the last paper?
2. What are the resulting technological enablers that need scoping and investigating as a result of the process improvement and in order to minimise risk?
3. How to make the PSSC more efficient, maintain service levels, maximise compliance and mitigate any risks?
4. What technology changes need to be made to address the recommendations of the Deloitte report and the needs for process improvement?
5. What does the future Target Operating Model look like for the PSSC?

Report

What progress on process improvement has been made since the last paper?

1. Ultimately, we are aiming to review 100% of the processes within the PSSC to minimise organisational risk and ensure that all employees continue to receive the right service at the right time in the most efficient way possible.

2. 96 Priority 1 and 2 processes for the process improvement review have been identified within PSSC and subsequent work streams commenced to analyse and improve these processes. To date, 74 processes have been reviewed - 13 Defined Benefit Pension Scheme processes and 61 additional processes. Priority 1 and 2 processes which have been completed or are in flight include work streams with PSSC Projects, Payroll, People Changes, Systems and MI. Improvements include 38 SuccessFactors configuration changes and changes to ways of working to reduce waste, remove risk and bridge process gaps. The advantages of using this method of change to SF means that these are all technically classed as minor changes which reduces the risk of any update issues in the future as they can easily be tested when mass updates are made and the configuration is easily manipulated to deal with changes meaning there is less incremental costs in the future.

3. The remaining processes will be subject to review throughout Q4 2020/1 with an objective to be completed at the end of Q1 2021/2 (see Appendix for high level plan). PSSC is working closely with Data Protection, Finance, Risk and Internal Audit to ensure that the necessary TrAction Controls are in place for each process as part of the review. Internal controls for all PSSC Managers have also been developed to ensure appropriate checkpoints throughout the processes.

4. Some role-based permission (RBPs) changes have been completed to facilitate the move towards one 'Tier 1' PSSC Team processing joiners, movers, leavers (JML), changes and queries. Process improvement reviews on work streams that support this model are in progress. This will drive improved efficiency through economies of scale and removal of single points of failure across basic administration processes. The ability to automate a number of these processes will reduce the risk of manual error, increase collaboration across teams through automation (e.g. IT) and improve the employee experience through more automated process and point in time interventions.

Strictly Confidential

POL00423694

What are the resulting technological enablers that need scoping and investigating as a result of the process improvement and in order to minimise risk?

5. Removal of the current risks associated with single points of failure within PSSC will be overcome by the ongoing enabling activity related to role-based permissions, and cross team training on SF activity relating to process work streams. This is being achieved by an iterative approach to the introduction of the revised processes and when the configuration changes to SF are fully tested and enabled.

6. Embedding the new processes and technology is a key driver to ensuring that risks are reduced quickly but due to the cyclical nature of some of the processes this is forecast to take some time and with the potential implementation of new technology through ServiceNow, it is forecast that risks will not be fully minimised until the end of Q3 2021/2. However, the current plan ensures that the more prevalent risks are being minimised first.

7. SF enabling works to reduce instances of data being calculated and entered manually, multiple times will reduce the risk of human error which can result in incorrect processing (e.g. incorrect entries on SF and in documentation). These changes have all been undertaken as part of process improvement through our small changes process with our systems integration partner. Each change has gone through full testing by both our partner and in-house team and been subject to post implementation review to ensure that changes are working as planned and have no unforeseen consequences. This enabling activity will continue throughout the process improvement work with the objective to be completed by the end of Q1 2021/2.

How to make the PSSC more efficient, maintain service levels, maximise compliance and mitigate any risks?

8. We will continue the process improvement project during Q4 20/21 and into 21/22 to complete the review and (where appropriate) improvement of PSSC processes. Align PSSC target operating model to work with the wider People TOM (in progress) and the reviewed PSSC processes, ensuring the PSSC has the right people, in the right structure to support the People Team and the wider business. This will require a skills gap analysis within the team alongside T2 activity.

9. During Q4 2020/1, the remaining P2 process work streams have been prioritised in line with those that represent greatest risk for POL (predominantly payroll processes) and P3 work streams with greatest opportunity (based on effort/impact assessment).

10. Additional SF configuration, identified by Deloitte review and ongoing process improvement project that cannot be completed as part of existing support contract (due to time, cost, and complexity) is being scoped currently in order to secure funding in Q1/2 2021/2.

11. From the beginning of Q4 2020/1, we will be executing the plan to upskill and develop knowledge within PSSC Systems Team, to reduce reliance on third party support for SF enhancements (currently c.90% of SF change tickets are completed by third party partner). Target is for c.80% of change/enhancement tickets (not defects) to be completed in house by the end of 2021/2. All configuration changes which will be carried out in-house will be carried out in conjunction with SF best practice and with the same assurances and risk mitigations applied to ensure that future updates will not be impacted without appropriate

Strictly Confidential

POL00423694

testing. Funding may be required for formal training within team once the initial capability gaps and training schedule has been completed.

What technology changes need to be made to address the recommendations of the Deloitte report and the needs for process improvement?

12. Further work has also taken place to address the recommendations in the Deloitte Report. As a result, it has been identified that along with the process improvement work, Service Now HR module could be introduced as a complementary and integrated technology to SF. Implementation of ServiceNow as a service management tool could be used for reactive work across PSSC. This will overcome the current lack of transparency (for customers) and control (for PSSC Management Team) regarding ticket progress and resolution. The risk of tickets being missed, unsatisfactorily completed, or missing SLAs, which will be implemented as part of the project, could be minimised and stakeholders could have a clear overview of open activity, as well as a full audit trail of completed activity. This piece of work is currently being scoped and a business case being developed with a target submission date of the end of January 2021. Currently the risks identified through lack of transparency and control of tickets is being managed manually through checks and balances. This process although effective, is inefficient and can lead to human error.

13. The potential introduction of ServiceNow will mean that some processes will need to be revisited to ensure that maximum efficiency can be gained by using the technology available. Further process improvement is likely therefore to continue in Q2 2021/2 before regular reviews and continuous improvement becomes part of business as usual.

14. A business case is being developed in order to articulate the full cost of the change to ensure benefits delivered (e.g. change resources, related process change and tool roll out). Target submission date is the end of January 2021. This will be managed and reported on via the OE Portfolio and in alignment with TOM activities.

15. The introduction of the ServiceNow HR module and the end-to-end process reviews could enable a lot of the recommendations in the Deloitte Report to be implemented without the incremental spend in SF. However, some investment in configuration of SF which sit outside of the current small changes portfolio will enable the following:
    - People/compensation data: Allow additional pay data to be stored/calculated/pulled from tables, reducing risk due to manual calculation/data entry;
    - RBPs: Further work on RBPs, including the definition and creation of additional RBPs where necessary, to remove risk caused by single points of failure within PSSC;
    - New/enhanced workflows and notifications: Ensure right stakeholders are involved/informed throughout processes by leveraging SF workflow capability;
    - Optimise mass org change/restructure process: SF enhancements to ensure mass upload functionality works for POL and offline, upstream processes (i.e. OD work) enable this approach

16. This potential new technology will also ensure that c.50% of the Deloitte recommendations will have been implemented and if successful in gaining funding will be completed and embedded by the end of Q3 2021/2.

Strictly Confidential

POL00423694

17. Should the investment in ServiceNow not be available processes will be reviewed to ensure maximum benefits can be gained without the use of automation. This will not be as efficient as it could be with the automation and will mean some risks will not be fully mitigated but further review will need to take place to ensure mitigation benefits are maximised.

What does the future Target Operating Model look like for the PSSC?

18. Through the Organisational Effectiveness programme and as a result of process efficiencies, it has been identified that PSSC is able to reduce by 6 roles in Tranche 2. The business case for this will be coming to Board into January. These 6 roles have been identified through the analysis of capacity and the efficiencies already gained by the process improvements that have been embedded.

19. The wider People TOM work stream, in which the PSSC role reduction sits, continues to progress in line with the timelines set out for the whole Organisational Design project. The People work streams follows in Phase Three (rightsizing support functions) after Phase One (identifying what products we sell) and Phase Two (identifying how we sell them) are embedded. We therefore anticipate that the People work stream will dovetail into Tranche 3 – date TBD but before January 2022.

20. For this reason, we are proposing to be very clear in our Tranche 2 narrative for change in PSSC that we are proposing the headcount reduction of 6 roles is due to being over-resourced for current capacity only. We will ensure that the function is aware that more change is inevitable as we are still on the transformation journey. We hope to be able to manage this in a low risk method, anticipating that there may be some leavers who want to take up Voluntary Redundancy at this time.

21. Returning to the role of the PSSC in the wider People TOM, the commitment for the PSSC is to become the "engine room" of the People function, ensuring that all requests for HR support come through the engine model and are escalated according to a tiered system.

22. The tiered model of support becomes an embedded principle so that:
    - Tier 0 – Will be self-service through ServiceNow and the PeopleHub
    - Tier 1 – Will be transactional processing through a dedicated team in the PSSC e.g. workflow requests or contract extensions
    - Tier 2 – Will be more complex processing requiring technical knowledge and experience – e.g. payroll or pensions

23. The final core principle is the use of technology in order to continue to minimise risk and to maximise efficiency at all times.

Appendix 1

Strictly Confidential

POL00423694

Sample process improvement summary:

Process: BAU Leavers **Workstream:** From Projects to Transactional Team **Owner:** From Tracy Wilkes to Wendy Swindells

Current state

Summary of wastes/issues/risks/gaps

BAU Leavers are currently processed by a dedicated resource in the PSSC Projects Team, as opposed to a pool of resource for 'transactional tickets' (i.e. tier 1). This results in inefficiency and over-resourcing for the work required. The current processes administered do not fully utilise SF to a) ensure right first time processing, b) push a workflow that involves the right stakeholders at the right time and c) automate calculation and information flow.

Processing time/work analysis

Type:	Ad-hoc
Frequency:	c. 27 BAU (non SA) leavers p/month (excl. Xmas Temps)
Time per transaction:	c. 3.3 **direct** hours per ticket (based on current 0.9 FTE dedicated to this work)
Total time:	89 **direct** hours p/month (235 days p/a @ 65% utilisation rate)

Future state

Summary of improvements/changes

Future state process includes a revised 'leaver entry' screen in SF, to include guidance notes and mandate minimum information requirements, removing unnecessary fields. This drives an increased right for time rate when PSSC process leavers, avoiding rework for PSSC and managers (e.g. obtaining missing information and clarifying ambiguity). Voluntary leavers are better informed throughout the leaver process, with an automated 'leaver to do list' email when the process commences and timely 'exit processed' confirmation email from SF. Workload has moved to correct team to manage all 'transactional tickets' (Tier 1) once tier model is established. For sensitive death in service cases requiring Reward intervention as CoE, an automated workflow is been developed, removing reliance on Reward being informed manually (to go live in January).

Benefits (cost/non cost)

- Improved right first time, removal of rework and realisation of economies of scale to achieve time saving
- Reduced risk of calculation errors and missed stakeholder engagement steps
- Enabling step towards achieving a Tier 1 'Transaction Services Team', managing JML changes and queries

Timeline

Sponsor sign off	PLT overview	Unions engagement	PSSC overview	People Team heads up	Business/customer comms
•07/12/20	•30/11/2020	•N/A	•Jan 2021	•Jan 2021	•Jan 2021

Go live: Jan 2021 (ETA) **FTE time saving:** 0.8 FTEs p/a

2

Update of slides 13 and 14 from original pack that went to ARC showing what has been completed.

8.2

Summary of Activity Findings (Focus Areas – Determined by 'Value Add') – Updated as at 4th January 2021

The 22 opportunities identified by Deloitte as 'Priority' based on value add have been 'combined' and worked up into 14 'prioritised opportunities that will form focus areas for POL as the PSSC is developed (It should be noted these were not necessarily quick win or low cost to implement and some rely on further development of the People TOM - therefore implementation is staggered)

	Prioritised opportunity	POL Activity	Approx delivery date	Owner
1	Optimise System Role Based Permissions in SuccessFactors	Role Based Permissions are being reviewed alongside the process improvement work (new processes will be defined that will identify the optimum RBP set up). Some RBPs have already been updated and this will continue as part of the implementation	Q4 2020/1	Helen Rhodes (PSSC Director) has the responsibility for all of these actions
2	Improve People Data Configuration in SF	This is a mix of small changes and more complex development. Ongoing programme to update and make small changes through Accenture Support – requirements sit alongside incoming ad hoc 'fixes' and urgent requests	Q2 2021/2 and ongoing BAU	
3	Improve Advice Centre Tiered Structure	Recommendation for tiered Advice Centre Structure an output of the Process Improvement work – maximising use of technical solution to reduce incoming requests. Tiered structure will be implemented as part of OD T3 activity.	Q3 2021/2	
4	Development of System Knowledge Capabilities	Formal development for the SF internal support team now available through the SAP / Success Factors Learning Zone. Secondment opportunity advertised and began Jan 21 for a 3 month secondment to concentrate on the Systems Team upskilling	Q1 2021/2	
5	Review SF development / support contract	Accenture contract has been reviewed and support moved to India from Lisbon. Further review of contractual commitments and needs post upskilling of internal team	Q2 2021/2	
6	Build out the People/IT Systems Governance and Innovation Forum	Post PSSC TOM / T2- Current forum responsibilities to be reviewed to support governance for change requests, system updates and release management, moving key decision making and activity prioritisation in-house (needs to be in conjunction with point 5) and in line with the IT Support model	Q3 2021/2	
7	Automated System Alerts for Absences & Stage Warning	Complex triggers at POL make automated alerts impossible. However, a new solution has been agreed with Employee Relations, empowering managers to manage the process and making use of system 'pop up' messages and reminders to support (Trial planned from 01/10)	Complete	

Work started | On track | On Hold (due cost or priority)

Key control mechanism for monitoring performance, future development & BAU updates

1

Strictly Confidential

POL00423694

Summary of Activity Findings (NEW)

	Prioritised opportunity	POL Activity	Approx delivery date	Owner
8	Redesign Employee Relations operating model	Subject to completion of People TOM – Needs full scoping – AdvisorPlus is in the process of being extended until 2022 when it is believed that the DMB Franchise Programme will be further advanced leading to less volume to be integrated into PSSC. The HR module of SNOW will be a key enabler to drive this integration and to ensure case management and knowledge management is improved internally.	Q4 2021/2	Lee Kelly (Employee Relations and Policy Director)
9	Perform End to End Onboarding Review and introduce automation to contract production and vetting processes	New onboarding process to go live in January 2021. Contract review ongoing with Legal Services	Q4 2020/1	Helen Rhodes (PSSC Director) has the responsibility for all of these actions
10	Digitisation of Consultation Packs & Leaver Letters	Aiming to have packs digitised for end of Q3. Solution worked through for payslips, p45s and accompanying letters	Complete	
11	Introduction of a full suite of PSSC and wider People Team SLAs	This will form a key part of the implementation of the HR module of SNOW and the development of T3 PSSC TOM	Q4 2021/2	
12	GDPR qualification. Processes and data flow are impaired by an overzealous interpretation of GDPR	GDPR compliant, but practical changes to RBP (Point 1) forms a key part of the process improvement work. Compliance is key to the process improvement work and removal of perceived barriers has been key in the development of new processes.	Q4 2020/1	
13	People Team mapping to processes with clear RACI	This is part of the People TOM work on the back of the wider POM activity. Clarity has already been given in the changes to structure made as a result of T1 organisational changes and this will continue through T2 and T3.	Q4 2021/22	
14	Optimise the Payroll & Pensions processing cycle	P1 and P2 payroll processes identified and work on some P1 activity has commenced. Forms part of the process improvement work which is also filtering into Project Assurance	Q4 2020/1	

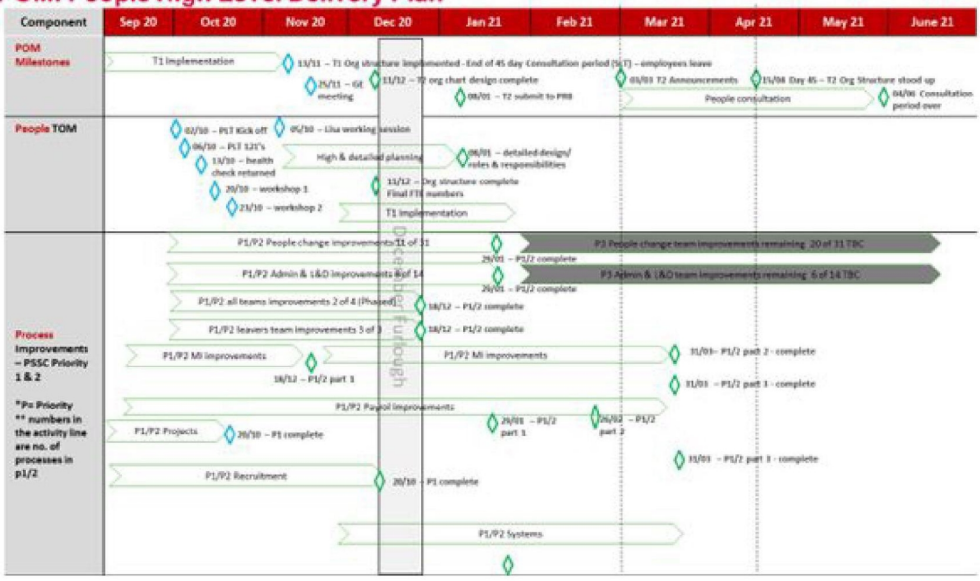
Work started | On track | On Hold (due east or priority)

2

High Level Project Level Delivery Plan

8.2

POM: People High Level Delivery Plan



7

Strictly Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Tax Update and Annual Tax Strategy	**Meeting Date:**	12 January 2021
Author:	Brian Kelly, Director, Treasury, Tax & Working Capital Andy Jamieson, Head of Tax	**Sponsor:**	Alisdair Cameron, Chief Finance Officer

Input Sought: Noting

The Risk & Compliance Committee (RCC) is asked to note the Tax Update and approve the annual review of the Tax Strategy for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

This paper is issued as a follow up to the paper presented to the RCC in January 2020. It provides an update on tax, as well as on the annual review of the Post Office Limited (POL) Tax Strategy last published in January 2020 (the "Tax Strategy").

Questions addressed

1. What are the strategic tax challenges for POL?
2. What are the current key tax issues for POL and what are we doing to address these?
3. What changes have been made to the tax team since the last update?
4. What other tax updates should the RCC/ ARC be aware of?
5. What is the requirement for reviewing and updating the published tax strategy?

9

Report

What are the strategic tax challenges for POL?

Improving controls around tax compliance

1. In the last few annual updates we reported that the primary tax risk was centred around VAT, however we have made good progress particularly enabled with CFS now being the single source of truth - it has allowed us to tighten controls and improve processes, reducing the risk of errors. In 2018 it took 5 to 7 days each month to pull together the VAT return information which would then be aggregated into the quarterly return. In 2020 it takes the same length of time to compile the whole quarterly return. The introduction of Web3 has also enabled us to bring in some automation in tax coding of purchases, further reducing risk, and providing more control for the tax team. We recently walked HMRC through Web3 and they were impressed with the controls and reduced risk.

2. It has become clear that we did not have sufficient expertise and knowledge in the business covering employment taxes. HMRC have expressed concern in the past over the lack of expert resource in this tax which has been evidenced by the disclosure earlier in 2020 and by the number of projects which require specialist input as well as legislative changes introduced to IR35 (Off Payroll Workers). We have therefore recruited an employment taxes

POL00423694

specialist to work in the tax team and to support HR colleagues, who should be in post by 5 March 2021.

3. HMRC introduced the Business Risk Review + regime in 2019, with the first reports in 2020. The revised regime has provided greater detail as to HMRC's requirements regarding the evidence and behaviours they wish to see in order to categorise the risk rating of the business. The risk rating determines how much audit focus HMRC places on the business and is used internally by HMRC to plan its interactions with businesses.

4. Risk is rated in three areas; Systems; Governance; and Approach to Tax Compliance. We were rated as low risk in approach to tax compliance, reflecting the work we have put in to reduce risk and tighten controls over the last year, however, we were rated as moderate-high risk for System and Governance due to particular concerns arising from the Horizon issues highlighted in the GLO (based on the public statements issued), the introduction of a new system, Web3, and error reporting in employment taxes. As more than one rating was in the moderate-high category this was also given as our overall rating. We have already provided reassurances over the integrity of Horizon and Web3 has brought reduced risk and we are recruiting an employment taxes specialist, all of which have helped to address HMRC's concerns. We therefore expect to achieve a lower rating in the 20/21 review to be reported on in April 2021.

Improving tax forecasting and maximising use of available reliefs

5. We have worked with Financial Planning & Analysis colleagues this year to build more accurate forecasting models for VAT and for corporation tax (CT). Historically our VAT position has remained very stable with little fluctuation on a year on year basis. However, the impact of Covid19 combined with the growth of Banking Framework income and the potential disposal of Telco have introduced variables which could significantly impact our VAT recovery rate, possibly reducing it by around 5%, with every 1% reduction giving us c.£500k additional VAT costs to bear. We have informed management of the possible impacts, based on our improved forecasting models and this on a monthly basis.

6. As the business has continues to improve its book profitability there is an increasing focus on management of corporation tax (CT). We continue to make tax losses, despite book profits, but we expect to be in a CT paying position in 22/23. We are therefore working to ensure we are able to make the best use of our historic tax losses (c.£1bn) which we have accumulated.

What are the current key tax issues for POL and what have we done to address these?

VAT

7. The primary VAT risk is to ensure that POL pays and claims the correct amount, this year we have focussed on;
   - ensuring our systems for reporting VAT to HMRC are compliant with Phase 2 of HMRC's Making Tax Digital requirements;
   - building system auto posting of tax codes into Web3 (the new purchasing system) and training staff;
   - and providing advice to the business regarding the revised Mails Distribution Agreement which contains several clauses relating to VAT charges between the two parties.

Systems/ MTD

POL00423694

8. We have used, and further refined, BI tools in VAT reporting to reduce manual intervention as per HMRC's requirements. This has in turn reduced the time in producing the VAT return and enabled us to focus more on checking and educating, rather than simply compiling the returns.

Web3 procurement system

9. We have also used the introduction of Web3 to remove the need for requisitioners to choose a tax code for buying an item or service, by auto populating tax codes against cost centres. We control and maintain the master list of tax codes. Not all cost centres can use the single rules, so there are occasions where manual over-writing is required, but this is the exception and not the rule. HMRC are currently undertaking an audit of the system, see para 26 below.

Mails Distribution Agreement 2 (MDA 2)

10. The original MDA contained numerous VAT clauses including a calculation clause which resulted in an annual payment, based on VAT transactions between the parties, c.£2.5m to Royal Mail Group (RMG). In MDA 2 we have replaced a substantial amount of the VAT clauses, removing the VAT calculation clause with a commercial settlement. This has reduced POL's financial risk as the general shift from letters to parcels increased the amount payable under the clause.

11. Both parties have worked to ensure that MDA 2 does not affect the VAT benefit arising from the special treatment of the income POL receives from RMG, referred to as the "Stamp Solution". As reported in the last update this provides an annual saving of c.£22m.

Post bill payment VAT treatment

12. In the January 2020 update we made the RCC/ARC aware of certain potential changes to the VAT treatment of commissions on bill payments. In June 2020 HMRC wrote to confirm VAT applies to this income, but allowing us to implement the change in our own time.

13. It is a complex project to amend the VAT treatment across, POL, Payzone and on our commission payments to Agents. We are on target for implementing the change with effect from mid-February 2021. The VAT change in income will impact our partial exemption VAT recovery rate, providing a c.£1m/ annum reduction in our overall VAT bill. There are very few clients which will be impacted by the change, i.e. most will be able to claim any VAT charged to them, in full, from HMRC.

14. We wrote to HMRC stating our intention to submit a historic VAT claim in relation to this issue. The claim would be based on the fact that, as there has been no change to our business operations, HMRC ruled on the VAT treatment of such supplies, therefore this treatment should always have applied. If we are successful, then reworking our partial exemption VAT recovery may provide a windfall cash repayment c.£3.5m. HMRC's initial response was that the claim would be valid, but we would have re-issue VAT invoices, and seek payment, covering the 4 year period of the claim to all clients. We are considering the practicality of this requirement and will decide in January after consulting with commercial and finance colleagues, whether to proceed.

Errors reported

POL00423694

15. We have identified only one VAT error this year which was a misclassification of income charged to RMG. This was cost neutral as RMG paid the outstanding VAT, leaving POL only with an interest charge to pay to HMRC of £50k. The billing template, in which the error arose, is being simplified and comprehensively reviewed during the change to the new financial settlement under MDA 2 which will further reduce the risk of errors.

Key Employment Taxes issues

Employees considered to have more than one permanent place of work

16. In 2019 we identified an issue whereby certain employees, who had been appointed on home-based contracts, were required to work regularly at office locations. Where there is a regular permanent second place of work and the individual claims expenses for travel, accommodation and subsistence, it is a taxable benefit-in-kind. HMRC deem the employee to have more than one permanent place of work. A payment in respect of tax was made for 19/20 as part of the normal annual settlement process and we disclosed an error and made a payment to HMRC of £403k for 15/16, 16/17 to 17/18.

17. Due to the impact of Covid19 there has been little travel in 20/21. We have provided guidance to HR colleagues regarding individuals who may require their contracts amending to reflect dual places of work and prevent additional tax being payable by the business, but at present due to the uncertainty changes have not been made. We continue to liaise and provide guidance to our HR colleagues on this issue.

IR35 – employment status of contractors

18. In 2017 HMRC updated IR35 legislation to assess whether roles filled by a contractor should be on the payroll or were a true 3rd party relationship. We are required to carry out assessments, using HMRC's online tool, when engaging contractors to assess their employment status. HMRC, although delaying the introduction of the new rules to the private sector, introduced a revised online assessment tool which must now be used to determine the employment status of contractors.

19. HMRC is currently carrying out a review of our application of the rules assessing a sample of contractors. There have been significant delays in the review due to Covid19. HMRC have asked for substantial additional information which we are collating to respond. We are comfortable that we applied the HMRC tests in a consistent manner in line with the guidance. Colleagues in the SPO are preparing the response to HMRC, to be sent in January.

Historic Settlement Scheme

20. Payments to claimants under the scheme may, in certain circumstances, be liable to tax and NI withholding responsibilities for us. We have been working with Deloitte and Herbert Smith Freehills to determine and agree the correct tax treatment and reporting mechanisms with HMRC. There are several different claim types which could be made in relation to different heads of loss. In order to cover the possible different tax treatments arising have built a matrix for the project team to ensure the correct treatment is applied to all claims.

Corporation Tax Losses

21. As at the 2018/19 tax year POL had accumulated tax losses of around £900 million. We estimate that, once the 2019/20 tax computation has been finalised and submitted, POL will have losses carried forward of in excess of £1 billion.

POL00423694

22. From April 2017 the utilisation of historic tax losses carried forward was restricted to a relief of £5 million against the initial profit and then a 50% restriction of any profits above £5 million. This means that POL will pay corporation tax sooner than it would have done under the old loss rules.

23. Despite being increasingly profitable at an EBITDAS level, POL continues to create tax losses whilst it incurs significant exceptional and transformational spend which is deductible for tax purposes. We have a built a model which is updated each period using the known funding amounts and income forecasts prepared by Financial Planning & Analysis colleagues. We do not anticipate paying corporation tax until 2022/23 at the earliest. Based on current income predictions the tax payable will be less than £3.5m.

What changes have been made to the tax team since the last update?

24. HMRC have previously indicated that, based on the size and complexity of the business, POL's tax team was under-resourced. We have now recruited a full-time Employment tax specialist team member to support the Head of Tax in this high risk area who is due to start at POL in early March 2021.

25. We undertook a tender for the provision of VAT and Corporation tax services in August 2020 and have appointed KPMG as our tax advisors. Deloitte remain as our Employment Tax advisors. We continue to take specialist advice where appropriate, based on the risk and complexity of the issues under consideration.

What other tax related issues should the RCC/ARC be made aware of?

Governance and Tax controls

26. The follow up to HMRC's 2016 Tax Governance report is still in draft, based on recent discussions we do not expect them to issue it until at least March 2021. The 2016 report highlighted a lack of documented process around tax and tax risk reporting. In the intervening period we have addressed each issue HMRC raised and informed HMRC of the improvements/ changes to processes we have made. We produce a quarterly tax summary report highlighting activity across all taxes which is circulated to the CFO, Head of Legal Services and the Group Chief People Officer. We also hold regular meetings with Risk colleagues and sign off tax controls, every month through PwC's 'TrAction' tool with supporting evidence uploaded into the system.

HMRC VAT Audit

27. New audits planned for 2020 were placed on hold due to Covid19. We have now agreed a program of more limited scope on-line audits which commenced in December with a walkthrough of Web3 and its interface with CFS using Microsoft Teams. HMRC reported they were impressed with the improvements we have made.

Making Tax Digital

28. Making Tax Digital (MTD) is a key part of the government's strategy to make it easier for individuals and businesses to get their tax right and keep on top of their affairs. HMRC's stated ambition is to become one of the most 'digitally advanced tax administrations in the world, modernising the tax system to make it more effective, efficient and to ease compliance'.

Confidential

POL00423694

29. We met the MTD requirements for Phase 1 in October 2019. We have also successfully met the Phase 2 requirements, which introduce the concept of requiring 'digital links' in VAT return supporting information. The deadline for compliance is 1 April 2021, meaning we are ahead of schedule. However, new compliance requirements stemming from Brexit cause concern and we are in dialogue with HMRC over this, see 29 below.

30. VAT is the first tax to be reported digitally to HMRC. In 2019 HMRC announced a delay to the introduction of digital corporation tax reporting, which was due from April 2020, but there is no official revised introduction date as yet.

Brexit

31. Due to the Government's requirements for electronic submissions covering the movements of stock from GB to NI, announced in November 2020, there are new reporting requirements being placed on the business. In addition, we will have to add VAT to the value of the goods moved and to claim back the some of this VAT in our VAT return and some in a later annual adjustment. These requirements are quite onerous and require new processes to be developed to in order to comply. We have contacted HMRC to see if there are any concessions available as there is no additional tax or Customs Duty payable by POL and have been told possible revisions to the new rules are being reviewed. We are concerned that the new system and reporting requirements will place undue burdens on the Tax team and may bring us into conflict with HMRC's Making Tax Digital requirements.

Tax Strategy – Annual Review

32. HMRC require that the POL Tax Strategy is reviewed, updated where required, and published on an annual basis. The initial Strategy was presented to and signed off by the ARC in November 2017. The Tax team has reviewed the current Strategy and have no proposed amendments as it remains fit for purpose and reflects our position and after sign-off will be published on the Corporate website and highlighted in a One News article.

33. The Tax Strategy is set out in Appendix 1.

Confidential

POL00423694

Appendix 1 – Post Office Group Tax Strategy

This publication sets out the tax strategy of Post Office Limited and its UK subsidiary undertakings (referred to hereafter as the "Group" or "Post Office") for the financial year 2021/22, and in making this strategy available the UK Group is fulfilling its responsibilities under the Finance Act 2016, Chapter 24, Schedule 19, Part 2, Paragraphs 16 & 17.

This tax strategy applies to UK taxes applicable to the Post Office and its affiliated entities both in the UK and overseas. The document is ultimately owned by the Board of Directors of Post Office Limited ("the Board").

The tax strategy is reviewed annually, updated as appropriate and approved by the Board each January to cover the next financial year. The Board, along with assistance from the Group Finance teams, take ultimate responsibility for setting, monitoring and amending the strategy as required.

In summary, the Post Office is committed to:

- following all applicable laws and regulations relating to its tax activities;
- continuing to have an open and honest relationship with HM Revenue & Customs driven by collaboration and integrity; and
- applying diligence and care in our management of taxes, and ensuring that our tax governance is appropriate.

How the Post Office manages its tax risks

The Group's on-going approach to UK tax risk management and governance is based on the principles of reasonable care and materiality. The Post Office maintains on-going application of tax governance, including frequent risk metric assessments and the review of applications of strong internal control procedures, in order to substantially reduce tax risk to materially acceptable levels.

As part of this governance, the Post Office has identified tax risks, which are maintained internally on risk registers, with their materiality being assessed based on a corporate risk matrix. The matrix then records the potential impact, subject to two contributory factors, the exposure if the tax risk crystallises and the relative likelihood of the risk crystallising.

Monthly review processes are carried out, based on the risk areas, and confirmation reports and evidence are logged in the external auditor's software. A quarterly tax issues report is then presented with significant / material issues to the Chief Financial Officer for his consideration, further discussion at Board level and with HM Revenue & Customs should the issue merit engagement of the tax authorities. Where decisions are deemed to be complex or have an element of uncertainty assistance from third parties may be sought to aid the Post Office's decision-making process.

POL00423694

Tax planning

Given that the Post Office is owned by the British Government's Department for Business, Energy & Industrial Strategy, it understands the importance of its transparent business operations.

The Post Office will not engage in artificial transactions the sole purpose of which is to reduce UK tax. As well as the above the Post Office will not engage in tax efficiencies if the underlying commercial objectives do not support the Group's position, or if the arrangements impact upon the Post Office's reputation, brand, corporate and social responsibilities, or future working relationships with HM Revenue & Customs.

Approach towards dealings with HMRC

The Post Office have always been and remain committed to maintaining integrity and transparency when dealing with HMRC. The Post Office underlines these principles by agreeing to:

- Accurately disclose all information required in correspondence and returns, and efficiently respond to communications as and when required. Where additional work is required, such as in the event of a disagreement, we will look to resolve this in the most professional and efficient way possible.

- Be open and transparent about decision-making, governance and tax planning, firstly by ensuring that it is liaising directly with our dedicated HMRC team and secondly by publishing our tax strategy easily accessible within the public domain.

- Ensure all interactions with HMRC are conducted in an open, collaborative and professional manner.

Signed

Alisdair Cameron

Chief Financial Officer and Senior Accounting Officer

(Updated January 2021)

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Update on balances posted to Postmaster accounts	**Meeting Date:**	12 January 2021
Author:	Tim Perkins, Service and Support Optimisation Director	**Sponsor:**	Amanda Jones, Retail and Franchise Network Director

Input Sought: Noting

The Risk & Compliance Committee (RCC) is asked to note the update on balances posted to Postmaster customer accounts following a request at the Audit, Risk & Compliance Committee (ARC) in September 2020, for onward submission to the ARC.

Previous Governance Oversight

Previous paper to ARC on 22nd September 2020

Executive Summary

The performance improvement reported to the ARC in September 2020 on branch balancing has continued through to week 38 of this financial year and each trading period of the current financial year has seen a year on year improvement.

Taken at a branch level, this means that the average branch has reduced its losses from £135.96 per trading period last financial year to £63.44 per trading period this financial year. This represents an annualised improvement per branch of £870.24.

The drivers of this performance are:

- Improved support for branches;
- Improved Post Office processes; and
- Lower transaction volumes during the Covid-19 pandemic

10

The improved branch balancing performance has resulted in lower balances being posted to Postmaster accounts. However, recoveries continue to be lower than balances posted to Postmaster accounts and this means that the total balances held on Postmaster accounts continue to increase.

A new policy has been developed to support the new processes being deployed by the Postmaster Account Support Team and this is detailed in a separate ARC paper on Postmaster policies.

To continue to improve performance in relation to branch balancing, Post Office will continue to find better ways to support branches with their branch accounting and to improve its own processes where they impact branch accounting. Post Office will also look to use data mining to identify the propositions and processes that most impact branch balancing.

Confidential

POL00423694

Questions addressed

1. Since the last update to the ARC in September 2020, what trends have been identified in balances posted to Postmaster accounts?
2. What progress has been made on reducing branch losses and balances posted to Postmaster accounts?

Report

1. The aim of this paper is to provide a more comprehensive overview of balances posted to Postmaster accounts and to update the ARC on the methods being deployed to reduce balances posted to Postmaster accounts.

Branch Accounting Processes

2. Post Office branches complete branch accounting known as branch balancing, a Trading Period or a Trading Statement on a periodic basis. The branches are split into four balancing groups, which means that in a four week trading period, different groups of branches balance in each week and in a five week trading period, the same groups balance in each of the first four weeks of the trading period. Effectively each branch balances on a five-weekly, four-weekly, four-weekly basis.

3. The activity involved in completing branch balancing involves physically counting all cash and stock in a branch and comparing that to the balance of cash and stock calculated by Horizon. At this point, a branch will either balance (the physical cash and stock matches the Horizon generated cash and stock), have a gain (the physical cash and stock is greater than the Horizon generated cash and stock) or have a loss (the physical cash and stock is less than the Horizon generated cash and stock).

4. For a branch to be able to be 'rolled' into the next trading period, the branch needs to balance. So, where there is a gain or a loss, the branch can choose to:
    a. Add or remove cash from the branch (known as settling to cash)
    b. Add a cheque to the branch (known as settling to cheque)
    c. Post the balance to the Postmaster's customer account (known as settling centrally)
    d. Post the balance to a nominee account if they are a multiple partner with a central account (known as settling to nominee)

5. The separate paper on Postmaster policies to this Committee details the new policy for managing and investigating balances posted to Postmaster's customer accounts.

Branch Balancing Performance

6. The last update to the ARC on Postmaster accounts in September 2020 reported that the number of branches experiencing losses when completing trading period accounting was falling and that the average value of losses experienced by the branches who had losses were also falling.

7. This pattern of lower branch losses and lower balances being settled to Postmaster accounts has continued through to week 38 (week commencing 14th December 2020).

Confidential

POL00423694

8. The following table shows the balancing results to week 38 this financial year versus the balancing results to week 38 the previous financial year:

Financial Year to Week 38	Gross losses	Gross gains	Net balance
FY2020-21	£16,951,639.52	£10,567,349.95	£6,384,289.57
FY2019-20	£25,549,872.16	£11,868,746.34	£13,681,125.82

9. This shows that the value of the gains and losses experienced by branches when balancing has reduced year on year.

10. For gains, the reduction is driven by a decrease in the average value of the gains with the average gain reducing to £356.13 from £437.67 (-18.6% YoY) and is partly offset by an increase in the number of gains from 27,118 to 29,673 (+9.4% YoY).

11. For losses, the reduction is driven by a decrease in both the average value of the losses from £749.44 to £556.92 (-25.7%) and the number of losses from 34,092 to 30,438 (-10.7%).

12. When also considering the ~40% of branches who balance exactly in a trading period, this means that the average branch is posting a loss of £63.44 per trading period this financial year versus a loss of £135.96 per trading period last financial year. This is an improvement of 53.3%.

13. The year on year improvement in performance is consistent, with each trading period of 2020-21 seeing an improvement year on year.

Drivers of Branch Balancing Performance

14. This performance has a number of drivers but it is difficult to precisely quantify the impact of each of the drivers.

15. Firstly, Post Office has purposefully and deliberately increased the level of support it offers to branches in relation to branch accounting.

16. There has been a focus to improve the level of compliance with trading period accounting and cash declarations across the network. This focus has seen Post Office make 8,211 compliance calls to branches to the end of Period 8 this financial year against 786 compliance calls in the same time period last year. Branch compliance has improved as a result with:
    a. the number of branches having not done cash declarations for over 10 days falling from 280 on 7th April 2020 (the first date this measure was established) to 36 as at Period 9, and
    b. the number of branches having not rolled over into the correct trading period falling from 104 on 7th April 2020 to 69 as at Period 9.
17. This improved level of compliance improves the reliability of the data used by Post Office to monitor the network and support Postmasters.

18. In December 2019, Post Office introduced a proactive intervention activity known as a SPEAR visit (SPEAR stands for Support, Prevent, Educate, Advise and Resolve). These visits

POL00423694

are pre-arranged and completed by the Audit Support team and are focused on helping branches who appear to be experiencing difficulties with their branch accounting.

19. There have been 518 SPEAR visits to the end of Period 8 and these have been supplemented by 311 SPEAR calls as a result of the Covid-19 pandemic. SPEAR activity is able to be completed with a shorter lead time than audit activity and requires less resource, so the level of responsiveness when a branch appears to be experiencing difficulties with their branch accounting is improved.

20. In April 2019, Post Office introduced a Tier 2 Balancing Support team into the Branch Support Centre. Tier 2 Balancing Support is a reactive support service that is in place to help Postmasters establish the cause of any gains or losses that they experience when balancing.

21. There have been 1,834 cases raised with the Tier 2 Balancing Support team to the end of Period 8. Cases are raised prior to a branch completing their trading period accounting (usually at weekly balancing or a cash declaration), so £3,172,975.80 of discrepancies that have been resolved by the Tier 2 Balancing Support team to the end of Period 8 will have directly contributed to the improved balancing results.

22. Secondly, Post Office has improved processes that support accurate branch accounting.

23. The volume of cash held in the network has reduced significantly year on year with average branch holdings at £39,167.91 at the end of Period 8 this year versus £43,576.14 at the end of Period 8 last year (-10.12%). This has been delivered through collaboration between the Supply Chain teams, the Area Manager team and the Network Monitoring and Support teams and was particularly key when releasing trapped cash from within the network during the first Covid-19 lockdown.

24. The reduced levels of cash in the network make cash handling easier for branches and allow the network monitoring teams to more easily identify branches with cash above the level expected for the branch.

25. Over the same period of time, branches with 'excess' cash of over £50k has fallen from 783 branches to 536 branches (-31.5%), with the value of the cash held at these branches falling from £84m to £53m (-36.9%).

26. The timeliness of the issuing of transaction corrections from the Branch Reconciliation Team has also improved. This is vital for supporting branches with reducing variability and maintaining accuracy in their branch accounting.

27. The number of items older than 2 months in the accounts from which transaction corrections are issued has fallen from 7,340 at the end of Period 8 last year to 1,447 at the end of Period 8 this year.

28. The improvement in the timeliness of transaction corrections is in spite of an increase in the volume of transaction corrections, which is being driven by cash pouch discrepancies.

Confidential

POL00423694

29. Training has also improved for branches in relation to branch accounting. Elearning modules have been introduced for ATM accounting, lottery accounting and basic balancing and classroom training courses have been introduced for completing basic transactions, completing basic balancing and investigating discrepancies. These specific training interventions are also supported with more on-site training for new and established Postmasters.

30. Thirdly, there will be an impact on balancing from the reduced number of transactions performed in branches over the last year due to the Covid-19 pandemic with fewer transactions having a direct link with lower levels of error resulting in gains or losses.

31. This is difficult to quantify, but on the basis that the number and value of gains and losses experienced by branches have remained lower than last year in the trading weeks where transaction volumes have been higher than last year, transaction volumes appear to be less of a driver of the improved performance than the increased level of support offered and the improvement in supporting processes.

Impact of Branch Balancing Performance on Postmaster Accounts

32. The result of the reduction in the value of the gains and losses experienced by branches when balancing is seen across all settlement options available to branches:

Financial Year to Week 38	Settled to cash	Settled to cheque	Settled centrally	Settled to nominee
FY2020-21	£316,657.22	£134,846.46	£1,323,629.42	£4,609,164.98
FY2019-20	£2,552,200.21	£177,177.05	£3,107,324.94	£8,329,234.55

33. For branches settling balances to cash, the average balance settled has fallen from £62.10 to £7.72 (-87.6%). For branches settling balances to cheque, the average balance settled has fallen from £411.08 to £395.44 (-3.8%). For branches settling balances to their Postmaster's account, the average balance settled has fallen from £1,042.38 to £526.50 (-49.5%). For branches settling balances to a nominee account, the average balance settled has fallen from £522.96 to £284.59 (-45.6%).

34. The reduction in balances settled to Postmaster accounts has, however, not resulted in a reduction in the total value held in Postmaster accounts. This is due to recovery levels continuing to be lower than the balances posted to Postmaster accounts (as has been the case since Post Office stopped automatically deducting balances held in Postmaster accounts from remuneration payments).

35. The new approach to managing balances held on Postmaster accounts is part of the Postmaster Account Support Policy being discussed at this ARC and the Group Executive will also spend time considering the approach to the increasing balances on Postmaster accounts in January 2021.

Further Improvements

36. The changes made by Post Office over the last 20 months have seen the branch balancing performance improve significantly. The levers of increased support and improved Post Office processes will continue to be the key levers in driving further improvements.

POL00423694

37. Post Office will continue to find better ways to improve branch accounting compliance, improve its monitoring capability, further refine the targeting of interventions, and improve the remote and face to face support it offers Postmasters with branch accounting.

38. Post Office will also continue to focus on targeted reductions in cash and stock holdings across the network, the speed of issuing transaction corrections and further improving the training proposition for new and existing Postmasters.

39. A review is underway within the Historical Matters Business Unit to look to remove the term 'settled centrally' from Horizon and the processes used at the end of a trading period. The term needs replacing to more accurately describe what a branch does when 'settling centrally', which is to move a balance, for investigation, to their Postmaster's account to allow them to begin the next trading period with a zeroed trading position. The review will also look to quickly remove the minimum value that can be settled centrally from £150 to £0.

40. There is also an opportunity to more deeply understand the root causes of accounting discrepancies through data mining, moving the detect and respond model currently used by Post Office to a predict and prevent model. Understanding the root causes will enable Post Office to understand which propositions and processes cause discrepancies and what corrective action is required to mitigate the causes.

Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Postmaster Policies	**Meeting Date:**	12 January 2021
Author:	Jo Milton, Senior Operational Improvement Manager	**Sponsor:**	Tim Perkins, Service and Support Optimisation Director and Amanda Jones, Retail and Franchise Network Director

Input Sought: Decision

The Risk & Compliance Committee (RCC) is asked to approve:

i. the three new Postmaster policies set out in the Appendices, namely:
   - Network Monitoring and Audit Support Policy;
   - Postmaster Account Support Policy;
   - Postmaster Accounting Dispute Resolution Policy;

ii. that, moving forwards, these policies be reviewed and approved annually by the RCC only;

for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

Following the Group Litigation Order (GLO), Post Office set about ensuring that its processes complied with the findings of the GLO.

The focus on processes has delivered a large number of changes to the support that Post Office offers postmasters over the last 20 months. However, this work has mainly been done without updating the policies that sit over the processes. This has often been the case because no policy existed in the first instance or the policy was so dated that it was irrelevant to the processes undertaken pre or post the GLO.

11

Having policies in place for the support Post Office provides postmasters will bring Post Office in line with best practice franchise businesses. The purposes of the policies are to provide guidance, set down principles and highlight risk areas, while also ensuring that Post Office is able to support postmasters effectively and compliantly with the GLO.

As part of an overall review of postmaster support policy requirements, this paper seeks approval for three new postmaster policies to reflect how Post Office will provide support to postmasters in relation to their branch accounting. There were previously no policies in this area.

Questions addressed

1. What policies are required to support the changes made to postmaster support following the GLO?
2. What policies have recently been developed and now require approval?
3. What further policy work is required to ensure there is a full complement of postmaster support policies in place and how will these be continually reviewed in the future?

POL00423694

Report

1. Following the Common Issues Judgment and Horizon Issues Judgment in the GLO, Post Office focused on improving processes to ensure compliance with the outcomes of the judgments.

2. Whilst process improvements were delivered, Post Office has identified that there was an absence of overarching policies for these processes to sit under. Where policies previously existed, they were often very aged and did not bear relevance to the processes that Post Office had improved.

3. As such, Post Office has set about developing a set of postmaster policies across key areas of postmaster support.

4. Post Office has identified that a comprehensive suite of postmaster policies is required to demonstrate and ensure GLO compliant support to postmasters in the following areas:
    a. Network Monitoring and Audit Support
    b. Network Cash and Stock Management and Transaction Corrections
    c. Postmaster Account Support
    d. Postmaster Accounting Dispute Resolution
    e. Postmaster Contractual Performance
    f. Postmaster Suspension
    g. Postmaster Termination
    h. Postmaster Appeals
    i. Postmaster Accountability
    j. Postmaster Complaint Handling

5. The policies relating to Contractual Performance, Postmaster Suspension and Termination are already approved and in use.

6. This paper seeks approval of the policies relating to Network Monitoring and Audit Support, Postmaster Account Support, and Postmaster Accounting Dispute Resolution. These policies can be found in the appendices to this paper.

11

7. The Network Monitoring and Audit Support policy sets out Post Office's network monitoring principles which aim to support postmasters with accounting practices, prevent postmasters from suffering discrepancies and protect both postmasters and Post Office from possible losses.

8. The Postmaster Account Support policy sets out how Post Office will notify postmasters pro-actively when an accounting discrepancy has occurred and how it will offer support to help postmasters understand the reason(s) for any discrepancy. The policy also sets out how Post Office could deal with the recovery of losses if the loss is established (following investigation and/or acceptance by the postmaster).

9. The Postmaster Accounting Dispute Resolution policy sets out how Post Office will investigate and resolve any accounting disputes raised by postmasters.

POL00423694

10. The remaining postmaster support policies identified above (Network Cash and Stock Management and Transaction Corrections, Postmaster Appeals, Postmaster Accountability and Postmaster Complaint Handling) will be presented to the RCC in March, along with an overarching postmaster support document that links all the postmaster support policies and processes.

Next Steps & Timelines

11. Following approval of the three policies, Post Office will ensure that:

- all relevant teams are fully trained on the new policies by the end of February 2021;
- the policies will be reviewed annually, for approval at RCC, beginning March 2021; and
- an overarching postmaster support document, linking all the relevant policies and processes, will be prepared for review by the end of March 2021.

Internal

POL00423694

Appendices

1. Network Monitoring and Audit Support Policy
2. Postmaster Account Support Policy
3. Postmaster Accounting Dispute Resolution Policy

Internal

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Mails Fraud Update	**Meeting Date:**	12 January 2021
Author:	Tim Perkins, Service and Support Optimisation Director	**Sponsor:**	Amanda Jones, Retail and Franchise Network Director

Input Sought: Noting

The Risk & Compliance Committee (RCC) is asked to note a mails fraud identified on 25th November 2020 through a whistleblow received by an Area Manager from a member of staff in an agency Post Office. The reported fraud involves branches processing mail items prior to the branch opening to the public, printing the mail labels and affixing them to the mail items and then switching off Horizon before the transactions are committed. The whistleblow related to this fraud being committed at three branches run by one Postmaster.

Executive Summary

Following a whistleblow from an assistant in an agency branch, Post Office has identified a method of completing a mails fraud where postage labels are printed in branch and used for delivery of postage items, but no payment for the service is made and there is no onward settlement with Royal Mail for the items.

Post Office has informed Royal Mail of the fraud and Royal Mail have indicated their intention to complete an investigation to gather direct evidence of the fraud, so that they can pursue the parties perpetrating the fraud. At the point of writing this paper, the dates for Royal Mail completing their investigation are not confirmed.

Post Office will implement a technical fix to prevent the fraud from being able to be completed once the Royal Mail investigation is completed.

Post Office have further investigated the potential for this type of fraud to be used on other products, but have not found any evidence that there are similar opportunities in other products.

However, given a number of significant frauds impacting Post Office in the last 24 months, a review into Post Office's fraud prevention capabilities will take place in Q4 2020-21. This review will make recommendations for fraud prevention enhancements to be made in 2021-22.

12

Questions addressed

1. How was the issue raised?
2. How is the fraud performed?
3. What steps have been taken to deal with the fraud?
4. What steps are being taken to prevent further fraud?

Report

1. On 25th November 2020, an assistant in an agency branch approached their Area Manager to report a suspected fraud being undertaken in their branch and in the other branches run by the Postmaster of the branch.

POL00423694

2. The assistant reported that two men entered the branch each morning and completed mails transactions on Horizon for mails items believed to have been collected from local businesses. The postage labels are printed in the standard way and affixed to the mails items before the men power down Horizon, leading to the items in the 'stack' being lost and unrecovered when Horizon is powered up again. The assistant reported that between 20 and 30 mails sacks were processed in this manner per day.

3. The Area Manager raised the assistant's concerns with the contracts and security teams for investigation.

4. A preliminary desktop investigation confirmed that the data held by Horizon tallied with the assistant's report of the method used to commit the fraud.

5. The preliminary investigation also confirmed that whilst the postage labels were produced, there is no corresponding sales record in Horizon for these postage labels. Given there is no sales record for the items, there is no subsequent settlement with Royal Mail for the service they still need to provide on the items.

6. This means that Royal Mail is the party that is most financially disadvantaged by the fraud. Post Office and the Postmaster will lose some commission from not settling the transactions with Royal Mail (assuming the transactions would otherwise be processed properly through the Post Office). However, if the Postmaster is taking some (non Horizon settled) payment for processing the mail items, the Postmaster will be gaining whatever payment they receive for processing the items.

7. Given the impact on Royal Mail, Post Office Security reported the issue to Royal Mail Group Security on 2nd December 2020, once the preliminary investigation had confirmed the method used to commit the fraud. Royal Mail Group Security indicated that they would be interested in pursuing the case and putting in place an operation that will gather direct evidence of the fraud being committed. In order to run such an operation, Royal Mail Group Security indicated that they would need authorisation and that any such operation would not take place until January 2021. Royal Mail indicated to Post Office Security that their favoured approach to investigations like this is to complete a full investigation and look to seek civil recovery from the fraudulent party. They reported recent success with this approach in relation to an eBay seller in the same geographical area as the branches highlighted to them.

8. At the point of writing this paper, Royal Mail have yet to confirm the date they intend to complete their operation to gather direct evidence.

9. Post Office decided not to immediately suspend the Postmaster of the three branches prior to the Royal Mail investigation being completed for the following reasons:
    a. Suspension of the Postmaster would likely impact the effectiveness of any Royal Mail investigation (as the fraudulent behaviour may cease),
    b. Suspension of the Postmaster may leave Royal Mail with no identified party to pursue for civil recovery (and recovery may fall on Post Office),
    c. Suspension of the Postmaster would be better done once direct evidence has been gathered through the Royal Mail investigation, and

POL00423694

d. Suspension of the Postmaster may impact the whistleblower.

10. Once the Royal Mail investigation is complete, Post Office will consider the evidence and make a decision on suspending the Postmaster at that point.

11. In addition to investigating the fraud being committed at the branches identified by the whistleblower, a review has been undertaken across the network to understand the prevalence of the fraud across the estate over the last 11 months.

12. This review found that 80.25% of the occurrences of labels being printed with no corresponding sales entry happened in 6 branches. 51.23% of all occurrences were in the 3 branches operated by the Postmaster at the whistleblower's branch.

13. The potential quantum of the potential fraud at these 6 branches amounts to £1,026,635.30 using the first class small parcel postage rate of £3.70.

14. In considering the method used in committing this fraud, Post Office have also looked at which other product types are 'non-recoverable' in the event of an unexpected Horizon shut down.

15. There are a number of other 'non-recoverable' products including stock items (such as stamps) and bill payment items. These other products are unlikely to be used to commit similar frauds because there is a consequential impact in committing the fraud:
    a. For stock items, physical stock would be short against Horizon generated stock and the branch wouldn't balance, and
    b. For bill payment items, the bill would remain unpaid and would generate a customer or a client query.

16. In order to prevent future occurrences of this type of fraud, Post Office is working with its suppliers to implement a technical fix to avoid the loss of the basket data if Horizon connectivity is disrupted. Post Office expects to be ready to implement this fix once the Royal Mail investigation is completed. If there is a gap between the completion of the Royal Mail investigation and the proposed implementation of the technical fix, Post Office will ensure robust monitoring is in place to identify any further frauds.

17. This fraud follows a number of other frauds that have had significant impact on Post Office in the last 24 months:
    a. A prepaid labels fraud where an operator inflated their commission by c£230k from Royal Mail by processing ghost prepaid labels,
    b. A Parcelforce reversals fraud where c£140k was identified as having been removed by a Postmaster's assistant from processing Parcelforce reversals where no corresponding sales were present, and
    c. A banking deposit fraud where a Postmaster was duped into making banking deposits of c£800k without the cash being introduced at the branch.

18. Whilst Post Office has responded to these frauds through increasing monitoring or implementing a technical fix (as is planned with the mails fraud), this approach is always reactive rather than proactive.

POL00423694

19. In order to move to a proactive position, Post Office will engage an external specialist to make an assessment of its fraud prevention capability and to run fraud penetration testing on products offered over Post Office counters.

20. This review will be completed in Q4 2020-21 and will recommend fraud prevention enhancements to be delivered in 2021-22. The initial review will be brought back to the RCC for oversight.

Stakeholder Implications

21. The main impacted stakeholder from the issue identified by this whistleblow is Royal Mail. The impact on Royal Mail is financial.

22. In order to mitigate the impact on Royal Mail and in order to approach resolution of the issue in a collaborative way, Post Office made Royal Mail aware of the issue immediately once it had confirmed the method of the fraud.

Next Steps & Timelines

23. There are a number of key actions as a result of the identification of this fraud:
    a. The completion of the Royal Mail-led investigation to gather direct evidence of the fraud. At the point of writing this paper, the date for completion of the Royal Mail investigation is unconfirmed.
    b. The Post Office response to the outcomes of the Royal Mail-led investigation. This will follow the completion of the investigation.
    c. The technical fix to avoid the loss of basket data for non-recoverable items if Horizon connectivity is disrupted. This will follow the completion of the investigation.
    d. The review of Post Office's fraud prevention capability and recommendations for fraud prevention enhancements. The review and recommendations are due to be completed in Q4 2020-21.

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Historical Matters Unit: Fraudulent Claims Controls & Delegation of Authority	**Meeting Date:**	12 January 2021
Author:	Graham Hemingway, Historical Matters Portfolio Lead	**Sponsor:**	Declan Salter, Historical Matters Director)

Input Sought: Noting

The Committee is asked to note how are risks relating to fraudulent claims being managed in the Historical Shortfall Scheme (and the Stamps Scheme) and that controls are in place to confirm the eligibility of claims for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

- 12th November 2020 – Risk & Compliance Committee (RCC) – Historical Matters Unit Governance Review
- 24th November 2020 – ARC – Historical Matters Unit Governance Review

Executive Summary

At RCC/ARC in November a review of Historical Matters (HM) Governance arrangements was presented and three additional actions were requested – this paper provides an update on these.

Context: The Governance arrangements relating to HM were outlined in papers to RCC/ARC during November 2020. Three areas were highlighted where further work was requested (24/11/2020 meeting minute reference below):

9.1 - Responsibilities, accountabilities and decision-making authorities (including the extent of delegation of authority) are to be clarified via completion of a RACI matrix.

- Discussions concerning UKGI/BEIS involvement in Historical Shortfall Scheme (HSS) approvals, which directly affects the operation of the schemes have continued during December and are expected to be finalised during January
- A verbal update will be provided to RCC and ARC relating to the latest position agreed as at the meeting dates

9.2 – What mitigations are put in place relating to the risk of fraudulent claims – and what controls are in place around eligibility of claims

- Fraud risks are being actively managed by Herbert Smith Freehills (HSF) and the Project team covering 21 separate fraud risks – see Appendix 1

9.3 – Data relating to fraudulent claims and eligibility to be appended to Criminal Cases Review Commission (CCRC) Board pack

- MI showing latest eligibility results (values and volumes) from HSS is already distributed as part of an MI pack that HSF share with to Board members on a weekly basis. (Eligibility extract attached at Appendix 1).

13

POL00423694

- Information relating to identification of fraudulent claims will be shared as part of CCRC Board packs from 14th January 2021.

Report

Fraud risks

The following key fraud risks and mitigations have been identified associated with different phases of HSS (see also Appendix 2 for further detail).

1. Letters to current/former Postmasters:
   4 risks (A1-A4 in Appendix 1) associated with communicating about the existence of HSS and inviting applications from the wrong persons/deceased persons
   a. Risks mitigated by use of internal HR addresses and external 3rd party address validation specialists
   b. Some queries received from former Postmasters who had moved multiple times and still received an invitation to join HSS indicate the correct people
2. Claim amounts exaggerated/inflated/inappropriate
   2 risks (D1, E1 in Appendix 1) associated with using information to 'game' or claim unreasonable amounts for heads of loss
   a. Risks mitigated by confirming quantum of claims is aligned to the quantum distribution (initially derived from a comparison of the quantum distribution for GLO claims, then further developed based on typical HSS claims) – exceptions are subject to additional scrutiny and review
   b. Additional risk mitigations to be implemented will involve processing claims in similar cohorts to limit the risk of sharing of information to game the decisions, or negotiate after an offer is made
3. Collaboration fraud
   a. 4 risks (F1, H1-H3) associated with potential claimant collaboration at Escalation or Mediation stage of scheme are to be partially mitigated by use of confidentiality clauses and by handling similar cohorts at similar times to limit information collaboration
   b. Additional mitigation is focused on agreeing negotiating limits with UKGI/BEIS in advance and limiting negotiation as appropriate
4. Payment fraud
   a. 3 risks (G1, G3-G4) associated with making payments to incorrect accounts are being mitigated by using standard checks when making payments, supplemented with additional checks to validate all bank accounts prior to making payment
   b. Additional checks are being made prior to making offer/payment to ensure payees are not on sanctions lists etc. which would mean payments could not be made

Eligibility controls

The following key checks are in place to confirm eligibility (see also Appendix 2 for further detail).

5. Claims from claimants who are not entitled to make a claim
   a. Bankrupt claimants – Risk partially mitigated via: asking claimant to confirm bankruptcy status in initial claim questionnaire; additionally partially mitigated by checking bankruptcy status with Official Receiver prior to starting to process a claim; and additionally partially mitigated prior to making an offer.

POL00423694

b. Company claimants – Risk mitigated by requesting full evidence of authority to act and supporting documentation
c. On behalf of deceased or incapacitated claimant – Appropriate documentation to be obtained to confirm authority to act

6. Claims from claimants outside of Scheme eligibility period
   a. Dates to which claims relate are confirmed as relevant to the use of HNG-X and directed to BAU processes if appropriate (e.g. claim relates to current version of HNG).

Additional checks to be used to confirm controls are being followed

7. In addition to the above standard risk mitigations, a random sample (no. to be agreed with Internal Audit) of claims will be subject to a monthly 'deep dive' to investigate if all process steps have been followed and all relevant evidence is available to substantiate the claim as required.
8. The results of the 'deep dives' to be reviewed at HM Committee and summarised to Board in monthly reports

Additional review of fraud risks and eligibility controls

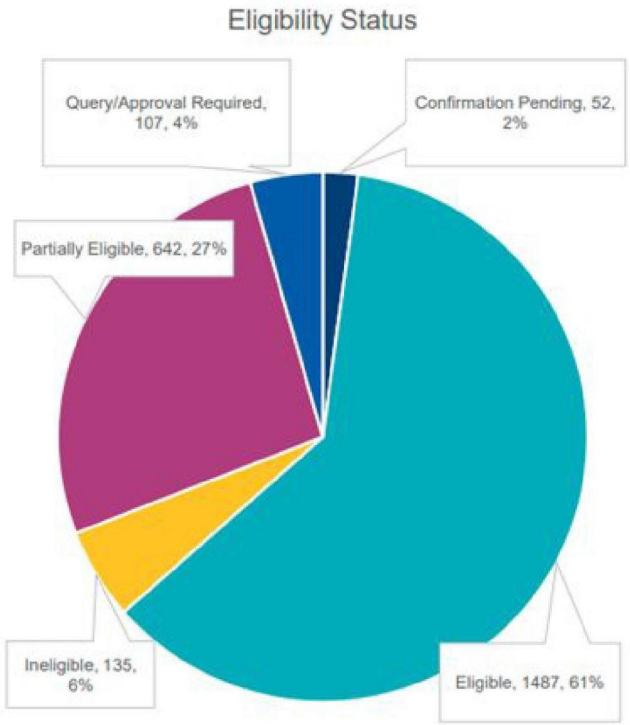
9. As a follow-up to Internal Audit review, an additional review of scheme fraud risk mitigations and eligibility controls will be carried out to determine and address any gaps.

Strictly Confidential

POL00423694

Appendix 1 – HSS Eligibility MI – provided to Board on a weekly basis by HSF (example from 2/1/21)

1.Total value claimed (Fully Quantified)	**£7,727,514.60**
(a) Ineligible	£384,586.64
(b) Eligible, yet to be determined, query	£7,342,927.96
2. Total value claimed (Part Quantified)	**£105,330,537.26**
(a) Ineligible	£17,295,663.87
(b) Eligible, yet to be determined, query	£88,034,873.39
Total Value Claimed (Fully Quantified and Part Quantified)	**£113,058,051.86**
Ineligible	£17,680,250.51
Eligible, yet to be determined, query	£95,377,801.35



13

4

Strictly Confidential

POL00423694

Appendix 2

Phase	Sub-Process	Ref	Potential Fraud Risk identified	Fraud Risk Mitigations	Comments
Scheme Publicised	Letter/email sent to Current Postmaster address	A1	Letters could go to incorrect address, triggering an attempt at identity fraud	POL HR validated addresses for all current Postmasters – letters were sent to appropriate correspondence address only	
	Letter/email sent to Former Postmaster address	A2	Letters could go to incorrect address, triggering an attempt at identity fraud of a deceased person/ghosting	Historic addresses were validated using Experian 'Address validation' software to identify changed addresses and/or changed names (e.g. marriage). Only addresses with appropriately high level of validation scoring were used	
		A3	Letter/email sent to deceased former Postmaster	Postmaster names/addresses were checked against Experian deceased person lists, to exclude those who had a high deceased score	Letters were sent to Postmasters with lower deceased scores (i.e. some deceased indicators, but not conclusive), in order not to exclude potential claimants unfairly
		A4	Letter sent to person who has a historical prosecution that has not been overturned (and therefore not eligible to claim)	Scheme Terms of Reference make this ineligibility clear The list of all known Postmasters who have prosecutions not overturned was excluded from receiving letters	
Claim received	Application form received Signed ToR received	B1	Potential Bankrupt Claimants – claimant may not be eligible to receive settlement	Application form asks claimant to confirm if they are bankrupt or not and sign accordingly Terms of Reference make clear that current bankrupts are not eligible themselves to claim, but that the correct claimant should be the Trustee in Bankruptcy	
Eligibility Assessment	Initial Eligibility Assessment	C1	Potential Bankrupt Claimants – claimant may not be eligible to receive settlement	Searches carried out on The Register (of bankruptcies) and equivalent for Scottish and NI jurisdictions	Risk still exists that name changes/address changes may invalidate searches (i.e. Register is not kept up to date with latest addresses), but not paying to current bankrupts is partially mitigated
		C2	Claim made by an individual on behalf of a company or partnership without consent of other parties	Evidence of authority to bring a claim on behalf of a company or partnership will be sought from claimants	
		C3	Claim made by an individual on behalf of a deceased or incapacitated Postmaster	Full, appropriate documentation to be provided, dependant on appropriate jurisdiction, to confirm claimant has authority to act – See Table 1 below, which was approved by Historic Matters Decision Making Forum in November	For incapacitated claimants, HM Committee may agree exceptions following escalation Scottish and NI Legal advice being confirmed
Document Collation/ investigation		D1	Claims could include exaggerated, or unusual heads of loss quantums, as a result of fraudulent/spurious applications	"Reasonableness checks' (already used on Stamps Scheme) to identify standard correlations between shortfalls claimed and other heads of loss claimed, so that anomalies can be scrutinised	
Claim Assessment and requests for further information		E1	Assessments could be based on further information that seeks to 'game' the assessment, based on fraudulent/spurious supplying of information as a result of initial assessment decision criteria being circulated	The requirement to maintain confidentiality is part of process and signed up to by claimants	Confidentiality clause could be ignored, and decision criteria could be shared (e.g. via Social media)
		E2		Similar cohorts of claims are processed in similar timelines to avoid potential for information leakage influencing the assessment/further information processes	
		E3		Compare quantum of heads of loss with previous settlement figures (i.e. the 555 GLO claims) to establish 'normal distribution' curves and highlight claims outside of these for further scrutiny	
Decision making and Outcome		F1	Sharing information associated with Settlement Agreements, in contravention of confidentiality clauses – could lead to claimant groups challenging settlement amounts at either Good Faith, Escalation of Mediation phases	Confidentiality clause to be highlighted to claimants Where appropriate, similar cases (e.g. de minimis) to be collated and co-ordinated to minimise opportunity/impact of information sharing in contravention of confidentiality clause.	

Strictly Confidential

POL00423694

Appendix 2 ctd.

Payments	Current PMs:	G1	Risk of payments fraud if payments made directly to bank accounts etc.	Standard POL processes to be used for making payments via remuneration channel, rather than directly wherever appropriate	
		G2	Incorrect taxation treatment by PM	Standard POL processes to be used for making payments via remuneration channel – with tax calculations to be based on agreed approaches following tax advice being confirmed internally and externally with HMRC and professional tax advisors	
	Former PMs: Direct payment to bank account	G3	Fraudulent/incorrect bank account used to accept payment – accidental or interception of payment request sent by physical means	Standard POL processes to be adopted for making direct payments – Recent copy of Bank statement to be used as a check of bank account details Additional Bank account validation to be carried out by Experian	
		G4	Fraudulent/incorrect bank account used to accept payment – accidental or interception of payment request sent by email	Standard POL processes to be adopted for making direct payments – Recent copy of Bank statement to be used as a check of bank account details Additional 'per payment' Bank account validation to be carried out by using Bank Wizard by Experian	
		G5	Incorrect taxation treatment by PM	Standard POL processes to be used for calculating payments using remuneration system functionality to determine tax calculations based on agreed approaches following tax advice being confirmed internally and externally with HMRC and professional tax advisors	
Dispute Resolution Process	Good Faith meeting	H1	Collaboration regarding outcomes from Good Faith meeting to artificially strengthen claimant negotiation	Agreement of Good Faith approach and tolerances Co-ordination of similar claims where appropriate to minimise opportunity for collaboration	
	Escalation meeting	H2	Collaboration regarding outcomes from Escalation meeting to artificially strengthen claimant negotiation	Agreement of Escalation approach and tolerances Co-ordination of similar claims where appropriate to minimise opportunity for collaboration	
	Mediation	H3	Collaboration regarding outcomes from Mediation to artificially strengthen claimant negotiation	Confidentiality agreement at heart of Mediation approaches Agreement of Mediation approach and tolerances Co-ordination of similar claims where appropriate to minimise opportunity for collaboration	

13

Strictly Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Policy Update	**Meeting Date:**	12 January 2021
Author:	Reena Chohan, People and Policy Compliance Manager	**Sponsor:**	Jonathan Hill, Director of Compliance Ben Foat, Group General Counsel

Input Sought: Approval

The Committee is asked to review and approve the following updated policies;

i. Cyber and Information Security Policy;
ii. Employee Vetting Requirements Policy and the Postmaster & Assistant Vetting Requirements Policy;
iii. Investigations Policy;

and endorse the proposed actions for the business, for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

This paper provides a summary of changes that have been made to the policies below as part of their annual review process for the RCC to consider.

Questions addressed in this paper

1. Which policies were updated in this annual cycle review?
2. What updates were included and why?
3. What is Compliance's assurance view of the status / Minimum Controls Standards for each policy?

Which policies were updated in this annual cycle review?

In this review cycle the following policies were revised, reviewed and updated as per the annual review process.

Policy	Last Reviewed	Updates	GE Owner	Governance Approval Body
Cyber Security and Information Security Policy	Jan 2020	Minor Updates	Chief Information Officer	RCC & ARC
Investigations Policy	Sep 2016	Major amendments to the existing policy, which has been out of use for some time.	Group General Counsel	RCC & ARC
Vetting Policy	2017	Entire rewrite and division of the policy	Group Chief People Officer and Retail and	RCC & ARC

14.1

POL00423694

			Franchise Network Director	
Postmaster Policies X 3	New Policies	To be discussed in a separate paper sent to RCC by Tim Perkins.	Retail and Franchise Network Director	RCC/ARC

What updates were included and why?

A summary that identifies the changes and updates to the policies and statements have been added below:

Cyber and Information Security Policy:

The updates mainly consist of some rewording and updating of links/references where teams have changed but nothing has substantively changed within the policy.

Policy Compliance View

Control standards can be evidenced as working through the annual Internal Audit and Deloitte maturity assessment and COBIT controls assessment. These assessments provide a comprehensive review of the policy and controls stated within them to ensure compliance with the policy is being maintained at all times.

Investigations Policy:

The Investigation Policy has not been updated or been in use for some time. Whilst most internal investigations are conducted under local, subject-specific policies – such as disciplinary, or Dignity at Work - it is felt that there should be an overarching policy dealing with subjects that are not dealt with under such existing local policies.

Therefore this is a master Investigations Policy that brings back the principles of investigations for all other Group Policies that relate to it. Going forward there is going to be as part of the implementation process an Investigations Group being pulled together, which will consist of both the relevant Policy Owners where it is intended that they will review the underlying processes of the policy and the appropriate MI to ensure all Minimum Control Standards stated within the policy are being met consistently.

The former policy has been updated to:

a. Include detail on the processes and on responsibilities.

b. Provide that, where there are existing investigation procedures within other policies, they should be followed.

c. Define roles and responsibilities more, and specifically to have someone appointed with overall responsibility for the investigation, i.e., the Commissioning Manager, who is responsible for establishing terms of reference and identifying the policy, legal and regulatory requirements of the investigation, including any requirement for an investigation to be carried out under legal privilege.

d. Equally there would then be an investigator responsible for the actual investigation. Effectively they have delegated authority through the Commissioning Manager.

POL00423694

e. Included certain aspects as obligatory on the managers, including producing minutes of interviews and an investigation report.

f. Include minimum control standards

Policy Compliance View

As this policy has not been in use for some time the attestation on the policy performance will need to be made and carried out in the next annual review - some of the control standards are in place but some will need to be established soon and are currently under review.

Vetting Policy:

The Post Office Ltd Vetting Policy was last updated in 2017 and following an internal audit which took place in April 2020, it was identified that the policy did not reflect the current organisation nor how vetting is currently delivered. In addition to this there was limited reference as to how the various groups should deliver vetting or the use of the vetting matrix to define minimum vetting levels.

The Vetting Policy as written in 2017 covered Post Office employees as well Postmasters and their assistants. However, these parties are vetted by two very distinct processes delivered by different teams. The policy has now been split out into two separate policies (one for employee and one for Postmaster/Assistants) and both now reflect the approach to vetting, who undertakes it and outlines the minimum vetting levels.

This is an entire rewrite of the policy.

Policy Compliance View

Given that this policy has been out of scope for some time the attestation on the policy performance will need to be made and carried out next year.

There are gaps to be addressed but these will need to be dealt with separately and is something the incoming Postmaster Effectiveness Director and Postmaster Onboarding Senior Manager will need to review and address. The fact that under the new structure Postmaster Onboarding and Assistant Vetting will sit in the same space (both working to the Postmaster Onboarding Senior Manager) should make these gaps easier to address.

Postmaster Policies:

To be discussed and approved in a separate paper present to the Committee by Tim Perkins.

Approval is being sought for three new postmaster policies to reflect how Post Office will provide support to postmasters in relation to their branch accounting.

The policies are:

- **The Network Monitoring and Audit Support policy** sets out Post Office's network monitoring principles which aim to support postmasters with accounting practices, prevent postmasters from suffering discrepancies and protect both postmasters and Post Office from possible losses.
- **The Postmaster Account Support policy** sets out how Post Office will notify postmasters pro-actively when an accounting discrepancy has occurred and how it will

POL00423694

offer support to help postmasters understand the reason(s) for any discrepancy. The policy also sets out how Post Office could deal with the recovery of losses if the loss is established (following investigation and/or acceptance by the postmaster).

- **The Postmaster Accounting Dispute Resolution policy** sets out how Post Office will investigate and resolve accounting disputes raised by postmasters.

Four remaining postmaster support policies will be presented to the RCC in March, along with an overarching postmaster support document that links all the postmaster support policies and processes.

Assurance

Working with the Policy Owner of the Conflicts of Interest Policy we have started to pilot the assurance process and sample test the policy on a risk basis to review the policy standard and policy compliance.

Compliance is also working with Policy Owners and our subsidiaries to incorporate where and whom their policies apply to within the business to ensure we have a consistent approach to the language that is being applied to all policies throughout the group.

The Internal Policy Template which is used by policy owners to draft their policies on, is currently under review and being amended to reflect current working practices as the previous one is outdated. The new template will include guidance notes for policy owners to help assist them in writing their policies. This is to ensure we have a consistent approach to policies been written and aligned in the same format throughout the Group.

Conclusion

We continue to work with Policy Owners and Company Secretariat to ensure we maintain our policy governance responsibilities and undertake assurance that the polices are working as expected. This is a key part of the wider Post Office controls work.

POL00423694

Appendices

1. Cyber & information Security Policy (Clean)
2. Cyber Security & Information Policy (Track Changed)
3. Employee Vetting Requirements Policy (Clean)
4. Postmaster & Assistant Vetting Requirements Policy (Clean)
5. Staff and Postmaster Vetting Requirements (Existing policy)
6. Investigations Policy (Clean)
7. Investigations Policy (Existing Policy)

Please see separate paper for the Postmaster Policies.

POL00423694

POST OFFICE LIMITED
RISK, & COMPLIANCE COMMITTEE REPORT

Title:	Subsidiary Policy Mandate	**Meeting Date:**	12 January 2021
Author:	Reena Chohan, People & Policy Compliance Manager	**Sponsor:**	Jonathan Hill, Compliance Director & Ben Foat, Group General Counsel

Input Sought: Decision

As part of our developing policy framework, the Committee is asked to review and approve the Subsidiary Policy Mandate, being:

i. Subsidiaries must adopt all Group Policies unless it cannot do so for a legal, regulatory or other material reason.
ii. Where subsidiaries cannot adopt a Group Policy for one of the above reasons, subsidiary shall adopt its own policy in that area that is aligned to the Group Policy.
iii. This adapted subsidiary policy must be reviewed and approved by the Post Office Limited (POL) Compliance team and the POL Policy Owner, who shall confirm alignment to the Group Policy.
iv. This process would not apply to Post Office Insurance (POI) regulatory policies, being Risk, Conduct Risk, Vulnerable Customers, Ex Gratia, Remuneration and any other policies as required by the Financial Conduct Authority (FCA). Where these policies are adopted by the POI Board, the Company Secretariat shall notify POL Compliance of the adoption such that their records can be updated;

for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

This paper provides a summary of the proposed actions for the Committee to consider with regards to the adoption of POL Group Policies by POL's subsidiaries: Payzone Bill Payments Limited (PZBPL) and POI.

PZBPL are currently undertaking a review of their policies and identifying gaps against the Key Policy Framework. Where there are gaps, they are either adopting the Group policy or drafting a new policy to align with the Group Policy but removing elements that are not applicable to PZBPL. In both instances, the policies are presented to the PZBPL Board for adoption (Group Policies) or approval (PZBPL policies adapted from Group Policies).

The PZBPL Board questioned whether the amended policies aligned with Group Policies given that PZBPL is ultimately overseen by the POL Audit, Risk & Compliance Committee (ARC) and what assurance could be given that this is the case.

POI have also been engaged in this work to ensure the approach can be aligned across the Group insofar as possible given POI's regulated status.

Accordingly, a Subsidiary Policy Mandate is proposed to resolve this query as well as give assurance to the ARC that POL's subsidiaries is adhering to Group Policies insofar as possible.

POL00423694

Questions addressed in this paper

1. What is the Policy approach for our subsidiaries?
2. How can we get alignment and consistency for Payzone?
3. What are the next steps?

The Report

What is the Policy approach for our subsidiaries?

1. There are currently 28 Group Policies that relate to Post Office's key risks. Each of these Policies have been established to set the minimum operating standards relating to their business area.

2. All of POL's subsidiaries should be required to adopt the Group Policies on a "comply or explain" basis i.e. they must adopt and comply, unless there is a specific regulatory, material or legal reason as to why they cannot.

How can we get alignment and consistency for our subsidiaries?

3. It is proposed that in cases where a subsidiary is unable to fully adopt Post Office Group Policies due to a specific regulatory, material or legal reason, the subsidiary will adopt their own policy in that specific area based on the Group Policy and there would be an approval process in place to approve and capture the variances/amendments being made to the policy in question. (*refer to appendix 1)*

4. This would apply to PZBPL in all instances. For POI, wherever possible the relevant Group Policy shall be adopted on a "comply or explain" basis. However, for policies that fall under the scope of POI's status as a FCA regulated firm, it is not appropriate for POL to have oversight such policies ("POI regulatory policies"). These policies presently include: Risk, Conduct Risk, Vulnerable Customers, Ex Gratia and Remuneration, but would also include any future policies as required by the FCA. Oversight for such policies must sit with the POI Board and would therefore not be subject to the approval process. Only POI policies that are not associated with POI's regulated status would be subject to the proposed approval process (for example, the POI Procurement Policy).

What are the next steps?

5. When the relevant Group Policy undergoes its annual review, the POL Policy Owner shall be responsible for engaging with subsidiaries on the policy review to either;

   i. adapt the Group Policy such that the subsidiary can adhere to it and therefore adopt the Group Policy; or
   ii. ensure the adapted subsidiary version is reviewed and continues to align to the Group Policy as amended.

6. This will ensure that, where possible, Group Policies are fit for purpose for the Group and not just POL. This would not apply to the POI regulatory policies.

POL00423694

7. POL Compliance will also work to update the policy guidance on the intranet to reflect the Group approach.

Assurance

9. The process will provide subsidiaries and the ARC assurance that there is a clear governance structure and audit trail to demonstrate sign off and appropriate approval of any variances being made to the Group Policies as adopted by the subsidiaries. POL Compliance will also keep a clear record of where policies are adopted and where they are adapted, alongside a record of what variations have been made. This will be supported by the Company Secretariat who will notify POL Compliance of any POI regulatory policies adopted by the POI Board.

10. The usual policy summary paper provided to each ARC will include an update as to which policies the subsidiaries have adopted.

Conclusion

11. POL Compliance continues to work with the Company Secretariat to ensure our policy governance responsibilities are maintained and assurance is provided that the polices being adopted by subsidiaries are aligned to the Key Policy Framework.

12. This is a key part of the wider work on strengthening Post Office controls.

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Procurement Governance & Compliance Report	**Meeting Date:**	12 January 2021
Author:	Barbara Brannon, Procurement Director	**Sponsor:**	Alisdair Cameron, Group Chief Finance Officer

Input Sought: Noting

The Committee is asked to review the report, noting the Procurement Risk Exceptions submitted to the Post Office Limited Group Executive and Board since November 2020 and to consider and give direction in respect of the contracts in the Procurement pipeline which are high value and at risk of being awarded or extended non-compliantly.

Previous Governance Oversight

- September 2020 – Board Report
- November 2020 – RCC & ARC Report

Executive Summary

As a business in receipt of public funds Post Office Limited (POL) is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £189k.

The purpose of this report is to set out both breaches to Post Office governance and key controls around contracts and compliance to PCR regulation in the award of contracts.

The aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

In March 2020, Post Office Board requested prior approval of all Exceptions. This was revised in September 2020 to above threshold Exceptions >£189k only in a revision to existing governance. From November 2020 sub threshold exceptions will be submitted to the Group Executive for prior approval and reported retrospectively to RCC and to ARC.

A Procurement Risk Exception Note is required to accompany all Exception Requests and a Legal Risk note for requests >£189k.

POL00423694

Questions addressed

1. *How many and what types of procurement risk exceptions have occurred in the past quarter?*
   Since the last Board report at the end of November there have been two Procurement Risk Exceptions submitted to the Group Executive for approval.
   - Smith & Williamson – Professional Services
   - Grant Thornton – Professional Services

   We also have a lapsed contract with our auditors, PWC which is an internal governance breach. A compliant extension option exists to extend but they are currently working at risk preparing an audit plan for 2020/21 while commercial terms are negotiated.

2. *What are we doing about it?*
   Active reviews continue with Business Units with the highest values relating to non-compliance.

   Our overall non-compliance value has reduced from IRRELEVANT in July, IRRELEVANT in November and is now IRRELEVANT

   A visual breakdown on all Open incidents at 5/01/21 is available in Appendix 1. A further £2.2m of open risk is due to be closed by end February 2021.

3. *What is in the current Procurement pipeline which is high value and at risk of being awarded or extended non-compliantly?*

   a) **£200k pa.** **Cheque Processing for Postal Orders and Camelot.**

   A risk exception was submitted to Board in June 2020 to extend our cheque clearing services with Barclays for bulk cheque clearing for Banking framework remittances, and cheques accepted as a method of payment. Work is underway to tender this service.
   At the time it was noted that a second contract with Barclays to process postal orders and Camelot cheques was also due to expire in June 2021. The intent was to tender both services together this year.
   It has become apparent that the two services are materially different with PO and Camelot cheques presented against the Post Office Ltd bank account rather than cleared to our Banking Framework or Utilities client accounts. They are effectively processed as part of our corporate banking services, billed by Barclays alongside corporate banking and internally managed operationally by our Back Office Finance team.
   The Corporate Banking Services contract expires in March 2022 and is due to be retendered in Q3 2021. There are operational consequences for Post Office should we split the services across two banks and so Procurement are proposing to extend clearing for Postal Orders and Camelot cheques and include into the scope of the

POL00423694

Corporate Banking Contract. A discussion is underway as to whether Post Office Ltd should publish a notice of this intent.

b) **TBC - Common Digital Platform (CDP) Disaggregation.**

Rather than procure a like for like service for application support and development IT are using this opportunity to align CDP with the future IT strategy and disaggregating the service. Hosting is already in the cloud and will compliantly transfer to the Back Office contract before transferring to the POL CoE for Cloud in due course. Options for application support and development [tendering certain pieces, moving non-customer facing components compliantly into the existing Back Office Accenture contract, and insourcing some elements] are under review with IT and Legal.
At present the application support and development services are unlikely to have been completely retendered or moved to other existing PCR compliant contracts by December as proposed to GE and Board and there are concerns in respect of resourcing and funding.
The view, however, is that this will have been completely achieved before revised contract end date in June 2021. The vast majority (by value) is expected to have been completed by the end of January 2021 as set out in the original Board paper.

Conclusion

Risk Exceptions are subject to extensive internal governance, legal and risk review, in line with POL governance guidance on value and risk. This is reflected in the material reduction in the value of open risks over the past 3 years.

Individually, all large value non-compliant contracts have been reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate and/or available.

Executive support towards moving POL towards a more compliant footing is very strong, but equally as important there is extensive support towards the cultural change required to ensure that Procurement activities and outcomes will support longer term business strategies and we reduce commercial risk making our 3rd party arrangements fit for purpose.

POL00423694

Report

4. What are the potential consequences of non-compliant awards?
   a) Pre-contractual remedies overview: During a Procurement, an aggrieved party can seek an interim injunction suspending the tender or the implementation until the court decides on an outcome.
   b) Post-contractual remedies: The court can order an 'ineffectiveness order' rendering the contract void &/or can award damages.

5. Why are these incidents of non-compliance occurring, and what can be done about it?

   Non-compliant awards may be made for a number of reasons at the Post Office.

   a) Low value, time constrained or highly sensitive/specialist engagements are not uncommon.
   b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy and/or completion of large, and complex technical programmes of work to maintain or enhance services prior to a possible exit.
   c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
   d) Delays to public sector panels of suppliers becoming available. The Post Office makes extensive use of this low-cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.
   e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
   f) Disregard for, or lack of understanding of the regulations.

6. Why are we receiving this report?
   A decision to collate this information into a single location was taken in the Autumn of 2016. The aim is to track and improve our overall compliance and commercial results as an organisation, while also ensuring perceptions are accurate. However, it should be noted that it will facilitate timely responses to Freedom of Information requests which adds risk to the Post Office commercial landscape.

7. Are any of these breaches arguable on regulatory grounds or are they all breaches?

   A full explanation of the individual compliance breaches for direct awards over £189k [previously £164k & £181k] threshold is attached in Appendix 1. Each entry details the nature of, and the value of the breach. The threshold is altered every two years based on the FX rate between GBP and the Euro.

POL00423694

The Procurement Compliance Register does not at present give an indicative risk level attached to the award. This information is provided to the accountable executives under internal governance processes in the form of a PCR risk note before a contract above threshold is entered into, and if necessary, under Legal Privilege. In addition, all signatories to a contract have sight of the Risk note as part of the Contract Authorisation Form [CAF].

All entries are compliance breaches. A period of challenge applies to each PCR breach once an aggrieved party becomes aware or ought to have become aware. This risk finally expires at 6 years from the date of breach. The defensibility of a legal challenge is outlined within a Risk Note.

8. How many of the breaches were approved in advance and how many retrospectively?
All contracts entered into during this period were compliant with internal governance processes on contract and commercial review.

9. Why were the approvals given?
The rationale for approval is relevant to the individual service and is detailed within Appendix 1.

10. What were the unapproved, material breaches?
There were no unapproved, material breaches during this period.

11. Describe what you are doing about the breaches. Where we are in breach, do we have a plan to come back into compliance and over what time period will that plan take effect?
    a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with their key stakeholders. The maturity of this look ahead view does vary currently and is consistently a high priority activity within the team.
    b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are actively involved helping to advise and review options as thinking evolves.
    c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
    d) Each RCC member now receives a regular report on compliance within their business unit[s].
    e) A Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with GE sign off.
    f) Awards over £189k must have prior Board approval before being entered into.
    g) All Professional Services engagements must be approved in writing in advance by the CFO/COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
    h) Procurement provides training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and a new training module made

POL00423694

available on Successfactors. Ad hoc training sessions for interested Business Units are also run.

i) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.

j) A revised POL Procurement Policy and supporting processes is in progress giving more granular guidance.

k) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.

l) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

Risk Assessment, Mitigations & Legal Implications

12. As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £189k.

13. Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.

14. The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

15. Contract and financial governance policy and processes at Post Office are set by the Legal, Risk and Governance team with clear guidelines for staff availably on the Company Secretariat team intranet site. This sets out steps to be taken to obtain financial and contractual approvals prior to making a binding commitment to an external party. Non-compliance to internal governance processes are also captured within this report.

POL00423694

Appendix 1 - All Open Material Incidents

Date	Procurement Category	Function	GE Member	Supplier Name	Value	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
10/01/2018	IT Software	Retail & Franchise	Amanda Jones (interim)	IRRELEVANT		In flight	PCR OJEU level	IRRELEVANT
23/12/2019	PR	Corporate Affairs & Comms	Richard Taylor			Pending	PCR OJEU level	
27/03/2020	IT Software	IT	Jeff Smyth (interim)			In flight	PCR OJEU level	
29/03/2020	IT Software	IT	Jeff Smyth (interim)			In flight	Medium threshold	
29/03/2020	Media	Marketing & Brand	Emma Springham			In flight	PCR OJEU level	
29/03/2020	Marketing	Marketing & Brand	Emma Springham			None	PCR OJEU level	
21/05/2020	Supply Chain	Operations & Supply Chain	Alisdair Cameron			In flight	Medium threshold	
21/05/2020	Supply Chain	Operations & Supply Chain	Alisdair Cameron			In flight	PCR OJEU level	
25/06/2020	IT SaaS	Marketing & Brand	Emma Springham			Pending	Medium threshold	

Strictly Confidential

POL00423694

Date	Procurement Category	Function	GE Member	Supplier Name	Value	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
25/06/2020	Banking Services	Retail & Franchise	Owen Woodley	IRRELEVANT		Pending	PCR OJEU level	IRRELEVANT
25/06/2020	Banking Services	Retail & Franchise	Owen Woodley			Pending	PCR OJEU level	
10/07/2020	Public Affairs	Corporate Affairs & Comms	Richard Taylor			None	Medium threshold	
10/07/2020	Marketing	Marketing & Brand	Emma Springham			Pending	Medium threshold	
10/07/2020	Professional Services	Finance	Alisdair Cameron			Pending	Medium threshold	
02/11/2020	Auditors	Finance	Alisdair Cameron			Pending		
01/09/2020	Professional Services	Commercial	Owen Woodley			None	Medium threshold	
11/11/2020	Professional Services	Finance	Alisdair Cameron			None	Medium threshold	
16/12/2020	Professional Services	Commercial	Owen Woodley			None	Medium threshold	
						excluding Audit Value		

Strictly Confidential

POL00423694

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Law & Trends Report	**Meeting Date:**	12 January 2021
Author:	Sarah Gray, Group Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Noting

The Committee is asked to note the new or proposed material changes to laws and regulations since the last Risk & Compliance Committee (RCC), for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

There are 5 matters for the Committee to note (details of which are set out in the Appendix):

1. **European Commission publishes new (draft) standard contractual clauses**
   New standard contractual clauses have been published to address the new requirements arising from the ruling on the Schrems II case to ensure an adequate level of protection on data transfers. ICO has not yet advised whether to adopt this approach in a Post Brexit Environment. The DPA team will continue to monitor developments and report through the Law & Trends Forum as when there are further updates.

2. **Information Commissioners Office publishes new guidance on Data Subject Access Requests**
   Following public consultation, new guidance has been published to help organisations respond to the increasingly costly and time-consuming requirement to respond to subject access requests. The new guidance is a positive for Post Office and hopefully makes the process simpler when trying to manage the increased burden of responding to DSARs.

3. **London Interbank Offered Rate ('LIBOR') Transition**
   Market is transitioning away from the interest rate benchmark LIBOR to a preferred alternative in order to remove all dependencies by the end of 2021. Certain loans to which Post Office is party to, as borrower and as lender, contain LIBOR rates and these will be reviewed and amended before the end of 2021.

4. **Reintroduction of the Crown Preference**
   HMRC has become a second ranking preferential creditor in respect of certain taxes and therefore in the event of insolvency will recover debts owed to it ahead of some other creditors.

5. **Revenue and Customs Brief No.12 - VAT Treatment on Compensation Payments – Update**
   HMRC published its Revenue and Customers Brief 12 (2020) that introduced their new position on VAT treatment of contractual compensation payments. The result of this approach by HMRC will mean that most compensation, early termination and cancellation payments will be

POL00423694

considered as payments for supply and will be liable for VAT. The Appendix updates on work done thus far. Our review has shown that the previous GLO settlements are not impacted nor the MDA, BFA or HPBB agreements. We will keep this issue under review as we expect further guidance to be issued.

6. **Revenue and Customs Brief No.12 – VAT Treatment on Lease Breaks**
   Our review highlighted only one break penalty was paid between 1 October 2017 and 1 October 2020. Although VAT was charged, a VAT invoice will need to be issued accordingly.

Questions addressed

1. What new or proposed material changes to laws and regulations should the Committee be aware of?
2. What are the implications to the Post Office business?

Report

See Appendix.

POL00423694

Appendix 1

Law & Trends Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
1. European Commission publishes draft new standard contractual clauses ('SCCs')	As reported at RCC in September 2020, the Court of Justice of the European Union ('CJEU') issued a final judgment that invalidated the EU:US Privacy Shield Framework as a transfer mechanism for transfers of personal data to the US, however ruled that SCCs were to remain a valid mechanism of data transfer outside of the EU. The impact of the judgement was softened by the promise that the European Data Protection Board would modernise the SCCs so that they aligned with the General Data Protection Regulations ('GDPR') brought in during 2018.	On 12 November the European Commission published the long awaited new (draft) SCCs for the transfer of personal data outside the EEA. Once approved, companies a one-year grace period to implement the new SCCs . The new SCCs adopt a modular approach which enables data exporters and importers to select the clauses that are relevant to the types of transfers they engage in, with all major transfer situations covered. The main difference in the new SCCs is that they place a duty on the data exporter to document a transfer risk assessment in all cases, with no allowance made for low risk transfers.	At this time, it is hard to comment on the true impact of the new SCCs given the UK's official departure from the EU on the 31 December. The impact is dependent on whether the Information Commissioner's Office ('ICO'), the UK regulator, decides to adopt the new SCCs so that we remain aligned with the EU regulations in place or not. If the ICO decide to adopt these clauses, Post Office could be looking at another remediation exercise across its contracts to replace where the old SCCs were used, as well as documenting the transfer impact statements. This could be a very resource heavy exercise to complete. The ICO have published a statement that they are considering its position and will take a pragmatic and proportionate approach, however they have not given any idea of when they intend to make a final decision. It is important to note that this is an area that historically has not attracted fines from the ICO, instead a ruling that the appropriate documentation needs to be put in place.	The Data Protection team continue to work with the legal team to keep abreast of any developments and ensure these are built into any upcoming contracts. Further updates will be provided to the Law and Trends Forum as appropriate.	
2. Information Commissioners Office publishes new guidance on Data Subject Access Requests ('DSARs')	The right of access to one's personal data is a fundamental right under data protection law and since the introduction of the GDPR more people have been exercising this right. The ICO launched a consultation in December 2019 and received over 350 responses from organisations of all sizes and sectors.	The guidance does not seek to make wholesale changes but makes clarifications or provides further detailed guidance that is aimed to assist companies when responding to DSARs. There are three key developments in the new guidance: - 'Stopping the clock' for clarifications – organisations usually have 30 days' to respond to a DSAR, however the new guidance gives organisations the ability to 'stop the	The new guidance is a positive for Post Office and hopefully makes the process simpler when trying to manage the increased burden of responding to DSARs. The key for Post Office is to ensure it applies a consistent approach, whilst always considering the context of each DSAR individually.	The Data Protection team will ensure the guidance is implemented and are considering developing a pricing matrix should Post Office choose to request a reasonable fee for responding to excessive and unfounded DSARs instead of simply rejecting.	

Strictly Confidential

POL00423694

	Following this consultation, the ICO have now published new guidance on the Right of Access.	clock' when it is necessary for the organisation to seek clarification from the data subject on their request. The guidance provides that the deadline extends for the same amount of time as the data subject takes to provide the clarification; - Rejecting a 'manifestly excessive' or 'manifestly unfounded' request – organisations have always had the right to reject DSARs that are 'manifestly excessive or unfounded' in nature, however the new guidance gives more direction on when a DSAR would fall into those categories and emphasises that organisations should consider each request on its own merit and not take a blanket approach; and - Charging to respond to excessive, unfounded or repeat requests – the new guidance says that instead of simply rejecting an excessive or unfounded request, an organisation can charge a reasonable fee for replying. There is no guidance on what a 'reasonable fee' is but the organisation must ensure the reasonable fee is proportionate whilst considering a number of factors such as staff time and photocopying costs. The guidance encourages organisations to consider a consistent formulaic approach should it wish to charge a reasonable fee.			
3. London Interbank Offered Rate ('LIBOR') Transition	LIBOR is the London Interbank Offered Rate. It is a benchmark interest rate calculated to produce an average of the rates at which large banks can borrow money from each other. Currently, the interest rate in most commercial loans between companies and banks is calculated by reference to LIBOR. It is also widely used in many other financial products and is available in 5 currencies, including sterling.	The use of LIBOR is coming to an end because most banks are not funded by borrowing from each other and therefore LIBOR no longer reflects the market. LIBOR will cease to be in effect from 31 December 2021 and an appropriate replacement must be found. The recommended replacement for LIBOR in the UK is the Sterling Overnight Indexed Average ('SONIA').	Certain loans to which Post Office is party to, as borrower and as lender, contain LIBOR rates and these will have to be reviewed and amended before the end of 2021. Post Office's working capital facility from BEIS is currently being revised and the transition from LIBOR is under negotiation.	Over the coming months, the Legal and Finance team will review the relevant agreements and those that refer to LIBOR will be amended. The expectation is that commercial agreements will not be affected, but this will be checked and confirmed.	

Strictly Confidential

Post Office Limited - Risk and Compliance Committee-12/01/21

POL00423694

		SONIA reflects the average interest rates that banks pay to transact sterling overnight from other financial institutions. The key difference between SONIA and LIBOR is that SONIA is backwards looking and is calculated each day, whereas LIBOR is forward looking and is determined at the start of an interest period. Changes from LIBOR to base rate of interest are also being seen in the market.			
4. Reintroduction of the Crown Preference	Since 2003, when The Enterprise Act 2002 abolished what was known as the 'Crown Preference', HMRC has been an unsecured creditor in respect of all taxes owed to it on any basis in the event of insolvency of a company. HMRC's position as an ordinary unsecured creditor meant it came below preferential creditors and secured creditors with a floating charge in the order of recovery.	On 1 December 2020, the Crown Preference was implemented once again, brought into effect by the Finance Act 2020 amendment to the Insolvency Act 1986. The Crown Preference now makes HMRC a secondary preferential creditor for certain taxes (VAT, PAYE and Employees' National Insurance), meaning recoveries in insolvency will be allocated to these HMRC debts ahead of many other creditors. In turn this could reduce the amounts that can be recovered by floating charge holders and unsecured creditors, which may mean they are less willing to extend credit, especially for certain businesses with high VAT or PAYE liabilities. Those in the restructure space see this change as rather unhelpful in assisting companies in danger, as floating charge lenders are likely to lend less money given the smaller bucket of assets recoverable.	There is likely to be a larger impact on the supply chain where businesses might be looking to extend their credit facilities and have trouble doing so. This could lead to liquidity constraints, particular if facing trading headwinds. It could impact Post Office if those in its supply chain were to go insolvent in that it could receive less than it would otherwise. The following industries are the most likely to be impacted: - Recruitment; - Wholesale; - Importers/Exporters; - Construction; and - Manufacturing.	Post Office will continue to monitor any further developments in this area and provide updates where appropriate.	
5. Revenue and Customs Brief No.12 - VAT Treatment on Compensation	On 2 September, HMRC published its Revenue and Customers Brief 12 (2020) that introduced their new position on VAT treatment of contractual compensation payments. The updated position means that VAT is applicable for:	Until recently, HMRC typically took the view that as compensation or damages payments made under a contract were not consideration for a supply of goods and services, they were therefore outside the scope of VAT. Following two recent EU judgements, HMRC has now reversed this position, so that many compensation payments or	A review was undertaken of historic litigation matters to establish potential liabilities that Post Office might have considering the new guidance. The Legal Team liaised with Post Office's insurers and external property litigation lawyers to identify any potential matters. The insurers did not consider they had any settlement payments which would be caught	Post Office Legal and Tax have reviewed what we consider to be the high-risk areas. In line with most other corporates, Post Office intends to await the further guidance expected from HMRC before undertaking reviews into a wider group of agreements.	

POL00423694

Payments Update	(i) Liquidated damages – payments made under contractual obligation to compensate the other party on early termination; and (ii) Payments for breach of contract – contracts which terminate on specific events and provide for a compensatory termination fee. The reasoning provided is that circumstances for terminating are as a result of events envisioned when entering into the contract and are therefore consideration for the supply of goods and services when they occur.	early termination fees will fall within the VAT regime. As noted in the last report, work was to be undertaken to investigate whether Post Office had received or made payments that would now sit inside of VAT.	by the new guidance; insurance claims are typically excluded. Property litigation payments is the area likely to be most affected by the guidance. HMRC are due to publish more guidance on the property aspect of their decision shortly and once this has been published a decision will be made whether to instruct the external property lawyers to undertake a full review of Post Office's historic property matters. The new guidance was also considered in light of payments made arising from the Group Litigation ('GLO Settlement'): - The GLO Settlement is silent to VAT, hence the settlement sums payable pursuant to it should be construed as being inclusive of VAT. - Other settlements made during 2020 ('Further Settlements') are either silent like the GLO Settlement or provide expressly that the Claimant Postmasters shall be responsible for any tax on the settlement sums. On the above basis, no further payment is required to be made by Post Office in respect of VAT on the GLO Settlement or Further Settlements. The position on further settlements under the Historical Shortfall Scheme is slightly different. The matter is being considered by KPMG, and the preliminary view is that no VAT should be payable however they are giving the matter further consideration. A review was also undertaken on the following commercial agreements: 1. Mails Distribution Agreement ('MDA') 2. Home, Phone and Broadband Agreement ('HPBB') 3. Banking Framework Agreement ('BFA')	Further updates will be given at Law & Trends Forum as appropriate.	

Strictly Confidential

Post Office Limited - Risk and Compliance Committee-12/01/21

POL00423694

			The outcome of the above review found that in relation to the MDA and HPBB, VAT was recoverable and therefore if a contractual compensation payment were to be made, the commercial terms for both contracts cover the new VAT treatment. In relation to the BFA all activity was VAT exempt and therefore this change in VAT treatment is not applicable. This means there is no immediate concern for any of the above agreements.		
5a. Revenue and Customs Brief No.12 – VAT Treatment on Lease Breaks	As reported above, on 2 September, HMRC published its Revenue and Customers Brief 12 (2020) that introduced their new position on VAT treatment of contractual compensation payments.	In addition to the updates reported above, HMRC's change in practice also means that in the context of leases, where a break clause is exercised to terminate a lease, there will now always be a supply for VAT purposes which will be exempt regardless of whether the break fee amount is provided for in the lease. As with the above, there is general unhappiness about HMRC's decision, especially the retrospective aspect as previously reported.	Post Office as liaised with BNP Paribas, its property manager, to ascertain to what extent this would affect Post Office. A review was undertaken to identify the number of lease breaks and the value of payments involved. Given the retrospective aspect of HMRC's decision, the review went back to the start of October 2017. Following the review, it was found for all lease breaks actioned between 1 October 2017 and 1 October 2020, there was only one break penalty paid. Fortunately for Post Office, VAT was already charged on this penalty at £2,075. Due to a process failure this wasn't raised as a VAT invoice, however this will now be rectified.	Legal and the Tax team continue to liaise closely on the implications of Brief 12 and ensure the correct processes are in place for VAT invoices to be appropriately issued going forward.	

POL00423694

18

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	26 January 2021
Time:	08:30 – 11.30
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	**Invited Attendees:**
Carla Stent (Chair)	Sally Smith (Money Laundering Reporting Officer & Head of Financial Crime): Item 5
Ken McCall (SID)	Amanda Bowe (Post Office Insurance ARC Chair): Item 6
Tom Cooper (NED, UKGI)	Tom Lee (Head of Finance Financial Accounting and Controls): Item 7
Zarin Patel (NED) (First half an hour only)	Brian Kelly (Director - Tax, Treasury and Working Capital): Item 8
Regular Attendees:	Andy Jamieson (Head of Tax) – Item 8
Tim Parker (Group Chairman, POL)	Tim Perkins (Service and Support Optimisation Director): Item 9, 10 & 11
Nick Read (Group CEO)	Declan Salter (GLO Director): Item 12
Alisdair Cameron (Group CFO)	Graham Hemmingway (Historical Matters Portfolio Lead): Item 12
Ben Foat (Group General Counsel)	Tony Jowett (Chief Information Security Officer): Item 13
Andrew Paynter (Audit Partner, PwC)	
Sarah Allen (Senior Manager, PwC)	
Rosie Clifton (Manager, PwC)	
Johann Appel (Head of Internal Audit)	
Mark Baldock (Head of Risk)	
Jonathan Hill (Compliance Director)	
Rebecca Whibley (Senior Assistant Company Secretary)	
Hugo Sharp (Deloitte Partner)	
Apologies:	
Zarin Patel (NED) (from 09:00 onwards)	
Join Microsoft Teams Meeting GRO United Kingdom, London (Toll) Conference ID: 69U 753 133# Pin (if applicable): 58042	

Time		Item		Owner	Action
08:00 -08:30		Meeting with Internal Auditors and ARC Committee without Management present		Auditors	Discussion
08:30	1.	Welcome & Conflicts of Interest		Chair	Noting
08:35	2.	Policies		Jonathan Hill	Approval
		2.1	Summary Paper		
		2.2	Investigations		
08:45	3.	Previous Meetings		Chair	Approval
		3.1	Minutes (24 November 2020)		
		3.2	Action List		
		3.3	Draft Risk and Compliance Committee Minutes (12 January 2021)		

Strictly Confidential

POL00423694

18

POST OFFICE LIMITED

08:55	4.	Risk, Compliance and Internal Audit Updates			
08:55		4.1	Risk Update	Mark Baldock	Noting & Approval
09:05		4.2	Risk Appetite Statement: Legal & Compliance	Ben Foat & Jonathan Hill	Approval
09:15		4.3	Compliance Update	Jonathan Hill	Noting
09:25		4.4	Internal Audit Update	Johann Appel	Noting
09:35	5.	Money Laundering Annual Report		Sally Smith	Discussion & Approval
09:45	6.	Update from Subsidiaries: verbal update Post Office Management Services (ARC)		Amanda Bowe	Noting
09:55	7.	Annual Report & Accounts Update		Alisdair Cameron & Tom Lee	Noting
10:05	8.	Tax Update & Tax Strategy		Brian Kelly & Andy Jamieson	Noting & Approval
10:15	9.	Update on branch losses and balances on Postmaster accounts		Tim Perkins	Noting
10:30	10.	Postmaster Policies - Postmaster Account Support Policy - Postmaster Accounting Dispute Resolution Policy - Network Monitoring and Audit Support Policy		Tim Perkins	Approval
10:50	11.	Mails Fraud Update		Tim Perkins	Noting
11:00	12.	Historical Matters Unit: Fraudulent Claims Controls & Delegation of Authority		Declan Salter & Graham Hemmingway	Noting
11:15	13.	IT Controls Assessment		Tony Jowett	Discussion & Noting
11:30	14.	Any other business		All	Noting
Items for Noting *These items will not be presented to the Committee and any questions should be sent to the Secretary for submission to the author for response. Questions and answers will be recorded as appendices to the meeting minutes.*					
	1.	HR Matters:			Noting
		1.1	Pensions Controls	Lisa Cherry & Maxine Cross	
		1.2	Success Factors	Lisa Cherry& Helen Rhodes	
	2.	IT Update:		Jeff Smyth	
		2.1	Cyber Security	Tony Jowett	
		2.2	Joiners, Movers, Leavers	Tony Jowett	

Strictly Confidential

POL00423694

18

POST OFFICE LIMITED

	3.	Procurement Governance & Compliance	Barbara Brannon	
	4.	Law & Trends Update	Sarah Gray & Ben Foat	
	5.	Accountable Person	Tom Lee & Christine Kirby	

Items for approval via Written Resolution

These items will not be presented to the Committee and approval will be sought via Written Resolution to be signed by members prior to the meeting. Any questions relating to these items should be sent to the Secretary for submission to the author for response.

	1.	Policies for Approval:		Jonathan Hill	Approval
		1.1	Summary Paper		
		1.2	Cyber & Information Security		
		1.3	Employee, Postmaster & Postmaster Assistant Vetting Requirements		
	2.	Subsidiary Policy Mandate			

Next ARC Meetings:

- Annual Report & Accounts: Friday 26 February 2021 at 08:30 – 10:00
- Ordinary meeting: Tuesday 30 March 2021 at 09:00 – 11:30

both in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft via Teams.

DRAFT

Strictly Confidential